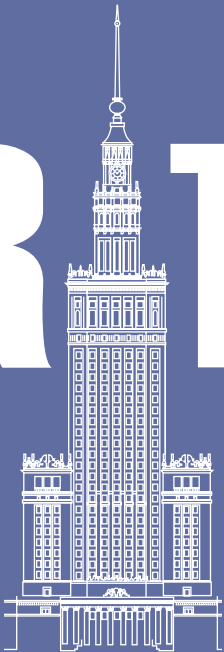


Katarzyna MANISZEWSKA, Paulina PIASECKA Editors

SECURITY AND SOCIETY IN THE INFORMATION AGE



Volume 3



Collegium
Civitas

Katarzyna MANISZEWSKA, Paulina PIASECKA Editors

SECURITY AND SOCIETY



IN THE INFORMATION AGE

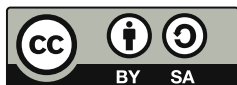
Volume 3

SRAS

Collegium
Civitas

COLLEGIUM CIVITAS

„Security and Society in the Information Age. Volume 3” publication is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License under the following terms – you must keep this information and credit Collegium Civitas as the holder of the copyrights to this publication.




To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/4.0/>

Reviews:

Daniel Boćkowski, PhD, University of Białystok

Marek Jeznach, PhD, an independent security researcher

Editors: Katarzyna Maniszewska, PhD ( <https://orcid.org/0000-0002-8021-8135>)

and Paulina Piasecka, PhD ( <https://orcid.org/0000-0003-3133-8154>)

Proofreader: Vanessa Tinker, PhD

e-ISBN: 978-83-66386-15-0

ISBN-print: 978-83-66386-16-7

DOI 10.6084/m9.figshare.13614143

Publisher: Collegium Civitas Press

Palace of Culture and Science, XI floor

00-901 Warsaw, 1 Defilad Square

tel. +48 22 656 71 96

e-mail: wydawnictwo@civitas.edu.pl

<http://www.civitas.edu.pl>

Cover design, typesetting and text makeup:

Ważka Łukasz Piotrowski

Contents

Dear Reader	5
1. Contemporary Conflict: The Role of Hybrid and Asymmetric Threats Matthew PIERRO	7
2. Active Cyber Defense and Operational Environment Preparation: An Opportunity for Progress Zoë BRAMMER	35
3. Shaping Future Internet Policy: Balancing Freedom and Security Through Globalization Sarah GOSSETT	50
4. The American Ape at the CIA: The Origin of Evolved and Learned Cognitive Mechanisms that Cloud Intelligence Analysts' Reasoning Steven DAVIC	72
5. Yea or Nay on Huawei? Altering the Balance of the 5G Technology War in Europe Jefferson T. STAMP	108
6. Threat Assessment of Chemical and Biological Warfare Lauren EDSON	125

7.	US and EU Counterterrorism Approaches: From Divisive to Convergent?	146
	Andrée WIETOR	
8.	Article 5 and the Challenges of Cyber Defense	164
	Theo WARNER	
9.	How Gun Policies Between The United States of America and the European Union Affect Modes of Violence Used by Far-Right Groups	177
	McKenzie KOTARA	
10.	The Relation Between the Refugee Crisis, Terrorism, and Far-right Extremism in Europe	191
	Sami SHIHADDEH	
11.	The Role of Disinformation in Migration: Case Studies of the United States and Sweden	203
	Marianne PERKINS	
12.	The Role of Sexual Offenses in Terrorist Activities	222
	Andrew M. HOLUB, Ph.D.	
13.	The Frequency and Influence of Far-Right Extremism in Current and Former American Military Personnel	238
	Kathryn WESTON	
14.	The Impact of Terrorism on Border Security in the EU: The Case of the Islamic State	247
	Yasmeen JONES	
	Bibliography	271
	Authors' bios	318

Dear Reader,

It is our pleasure to present a third scholarly volume bringing together a unique series of research papers by talented students – participants in the Security and Society in the Information Age program held at Collegium Civitas University in Warsaw, Poland.

In the 2019/2020 academic year, due to the pandemic, it was not possible for the students to physically come to Warsaw. Thus, for the first time, the program was held online. The students took part in a fully-fledged online course and an online research internship at the Terrorism Research Center.

The Security and Society in the Information Age program is organized in Warsaw jointly by Collegium Civitas and SRAS (USA). It is composed of summer school courses, semester or academic year abroad opportunities as well as an optional internship. The courses are devoted to a wide range of historical and security issues – with the region of Central and Eastern Europe serving as a case study. The courses are taught in English by academic experts and practitioners. The program is aimed at ambitious students who are eager to engage in and out of the classroom and want to enhance their competencies and boost their academic and professional careers.

The internship program is organized by the Terrorism Research Center (TRC) – a leading think-tank and research unit within Collegium Civitas. The main fields of activity of TRC include scientific projects, analytical undertakings as well as raising awareness about security issues in society. TRC focuses on a wide range of security challenges surrounding international terrorism and how to combat it. During the internship, students deepen their knowledge on selected security issues and embark on their own research project, supervised by mentors who are experts at TRC.

This scholarly volume presents the results of the internship held in 2020. The interns explored a variety of important security issues facing modern societies, including: terrorism, migration and disinformation, violent extremism and radicalization, border security, internet and security policies, intelligence analysis, cyber threats, biological and chemical warfare, and trade restrictions in 5G technology.

The contributions give an overview about selected, current challenges in today's interconnected world. The authors also looked for solutions and included recommendations for law enforcement, policy makers and scholars.

We hope you will find this book interesting and valuable and we cordially invite you to learn more about the Security and Society in the Information Age program at: www.securityandsociety.org

Dr. Katarzyna Maniszewska
Vice-Rector for International
Relations Collegium Civitas

Renee Stillings
Director
SRAS

Dr. Paulina Piasecka
Deputy Director
Terrorism Research
Center

Contemporary Conflict: The Role of Hybrid and Asymmetric Threats

Matthew PIERRO

Abstract: In recent decades, the international stage has witnessed warfare's evolution away from conventional tactics. Whereas historically rivaling nation-states dueled on rigid battlefields to declare a winning power, modern tactics have blurred the lines between war and peace while removing definite fronts, actors, and necessary capabilities. This is representative of modern-day asymmetric threats: used generally by weaker actors in conflict to exploit vulnerabilities in a more powerful opponent, these strategies circumvent direct confrontation while being unconventional, irregular, and difficult to combat. In unison with traditional war tactics, these characterize hybrid warfare which combines asymmetric and conventional aspects of conflict. This paper will examine asymmetric and hybrid threats, their status modeling conflict in the 21st century, and the actors, both state and non-state, that drive their use. Further, a variety of case studies will be examined from which recommendations to combat asymmetric and hybrid tactics will be made.

Keywords: asymmetric threats, hybrid warfare, state, non-state actors, conventional warfare, cyber attacks

Introduction

In the most elementary sense, warfare can be framed by the notion of opposition and the clash of opposing ideological blocs. This concept is neither new nor uniform: warfare has long been subject to evolutionary forces and its existence has been defined according to a variety of historical and present perspectives. Carl von Clausewitz, a Prussian general and military theorist active during the Napoleonic Wars,¹ provided several definitions of **warfare**: once as “*the continuation of politics by other means*”², while later as “*...nothing but a duel on an extensive scale...an act of violence intended to compel our opponent to fulfill our will*”³ and “*...a natural part of human life*.”⁴ This implication of warfare as state-dominated⁵ was a product of conventional tactics prominent in Clausewitz’s era. Nonetheless, to many, the prevailing perception of warfare is similarly conventional in nature. Military historian John Keegan proposed this in his **political-rationalist theory of war**⁶, saying “[warfare] is assumed to be an orderly affair in which states are involved, in which there are declared beginnings and ends, easily identifiable combatants, and high levels of obedience by subordinates.”⁷ Per Keegan, this theory deals poorly with non-state and non-conventional tactics, the subject of this paper⁸.

The rationalist theory finds company in academic literature. Jean-Jacques Rousseau, a Genevan philosopher and enlightenment thinker⁹, argued warfare as “*...a relation, not between a man and a man, but between State*

¹ Beatrice Heuser. *Reading Clausewitz*. London: Pimlico, 2002.

² Alexander Mosely. “The Philosophy of War”. Internet Encyclopedia of Philosophy. Accessed August 24, 2020. <https://iep.utm.edu/war/>.

³ Jordan Lindell. “Clausewitz: War, Peace and Politics”. E-International Relations, November 26, 2009. <https://www.e-ir.info/2009/11/26/clausewitz-war-peace-and-politics/>.

⁴ Ibid.

⁵ Alexander Mosely. “The Philosophy of War”.

⁶ Alexander Mosely. “The Philosophy of War”.

⁷ Ibid.

⁸ Ibid.

⁹ Christopher Bertram,. “Jean Jacques Rousseau”. Stanford Encyclopedia of Philosophy. Stanford University, May 26, 2017. <https://plato.stanford.edu/entries/rousseau/>.

and State.”¹⁰ Even Webster’s Dictionary, a supposed arbitrator of word usage, defines war as “a state...of conflict between states or nations.”¹¹ Conventional warfare fits within these classifications: global security has historically evolved around the clashes of nation-states and their militaristic ventures. The end of the 20th century and notably the Cold War, however, has demonstrated a dramatic shift in the sphere of conflict.

Witness to increasingly powerful nation-states with numerically extravagant armies and weapon arsenals, pure conventional warfare has lost its position as a viable means of completing political goals. As of January 2019, the United States military budget exceeded \$700 billion dollars¹². When accounting for inflation, this exceeds the Cold War average for the United States by over \$100 billion¹³. Boasting a military of this strength, conventional warfare with the United States is not a practical strategy. The disparity is blatant in the on-going conflict in Iraq: in 2019, Iraq’s military budget valued roughly \$6.7 billion in US dollars, a fraction of the resources wielded by the United States¹⁴. As such, counters to U.S. offensive attacks (such as the assassination of Iranian commander Qassem Soleimani¹⁵, asymmetrical itself) include mass demonstrations and a rocket attack on the U.S. Embassy in Baghdad¹⁶. In sum, warfare has been forced to adapt to the powers that participate in it. Nonetheless, warfare represents more than the individuals or weapons involved: it is the theatre in which oppos-

¹⁰ Alexander Mosely. “The Philosophy of War”.

¹¹ “War”. Merriam-Webster. Merriam-Webster. Accessed August 24, 2020. <https://www.merriam-webster.com/dictionary/war>.

¹² Miller, James N., and Michael O’Hanlon. “Quality over Quantity: U.S. Military Strategy and Spending in the Trump Years”. *Foreign Policy at Brookings*, January 2019, 1–9.

¹³ *Ibid*, 2.

¹⁴ “Iraqi Defense Market Outlook to 2024 – Iraqi Defense Expenditure Expected to Record a CAGR of 5.5% Over 2020–2024”. GlobeNewswire News Room. Research and Markets, December 16, 2019. <https://www.globenewswire.com/news-release/2019/12/16/1961172/0/en/Iraqi-Defense-Market-Outlook-to-2024-Iraqi-Defense-Expenditure-Expected-to-Record-a-CAGR-of-5-5-Over-2020-2024.html>.

¹⁵ Felbab-Brown, Vanda. “Stuck in the Middle: Iraq and the Enduring Conflict between United States and Iran”. Brookings. Brookings Institute, January 29, 2020. <https://www.brookings.edu/blog/order-from-chaos/2020/01/29/stuck-in-the-middle-iraq-and-the-enduring-conflict-between-united-states-and-iran/>.

¹⁶ *Ibid*.

ing values clash, and in modern society it has morphed into a path around the stalemate between powerful national armies.

Definitions: Asymmetric Threats

Referenced above, select nation-states dominate military spending (and generally global conflict). A prominent example is the United States, whose national defense budget constitutes nearly 40% of global military spending while their allies account for (roughly) another third.¹⁷ This accumulation of force proves counter to deterrent efforts: according to the Serbian *Report of the Quadrennial Defense Review*, released in May 1997¹⁸, U.S. dominance in the conventional military arena may encourage adversaries to use such asymmetric means¹⁹. Thus, the concept of **asymmetric threats** was introduced, proposed as *a strategy to avoid direct military confrontation with the U.S. or to disrupt U.S. commands, controls, communication systems, and alliances*²⁰. Steven Metz, an American national security expert at the U.S. Army War College²¹, critiqued this nation-specific definition and proposed a more complete definition of asymmetric strategy: “[in military affairs] asymmetry is acting, organizing, and thinking differently than opponents to maximize relative strengths, exploit opponent’s weaknesses or gain greater freedom of action.”²². Contrary to nation-states in the upper echelons of military spending, weaker sides in conflict must circumvent direct attacks in favor of unexpected tactics, due both to their own shortcomings and to the superiority of their opponent²³. These

¹⁷ James Miller, N., Michael O’Hanlon. “Quality over Quantity”, 2.

¹⁸ Milica Ćurčić. “Asymmetric Threats in Security Studies”. *Thematic Collection of Articles – Asymmetry and Strategy*, 2018, 17–29.

¹⁹ Ibid, 20.

²⁰ Ibid, 20.

²¹ “Steven Metz”. Strategic Studies Institute. US Army War College. Accessed August 24, 2020. <https://ssi.armywarcollege.edu/faculty-staff/author-bio-metz/?q=543>.

²² Milica Ćurčić. “Asymmetric Threats”, 21.

²³ Nikola Brzica. “Understanding Contemporary Asymmetric Threats”. *Croatian International Relations Review* 24, no. 83 (October 29, 2018): 34–51. <https://doi.org/10.2478/cirr-2018-0013>.

asymmetric approaches employ innovative, nontraditional tactics, and weapons or technologies that are irregular in nature.

Asymmetric threats vary across a multitude of platforms, including disinformation campaigns, terrorism, and cyberattacks. Importantly, these tactics exist under the threshold for conventional conflict while still destabilizing governments, alliances, or organizations²⁴. According to the Ministry of Defense in Serbia, certain characteristics are inherently asymmetric when:

1. considered unusual from a conventional point of view (i.e. torture);
2. irregular in the sense that they violate treaties or laws of armed conflict;
3. depart from war as previously understood, (as in flying planes into buildings);
4. leveraged or specialized against assets;
5. difficult to respond to proportionally, creating a situation where military intervention in response seems inhumane or cruel;
6. having unforeseen circumstances, typical of an event or attack not previously used²⁵.

Stephen Blank, a Senior Fellow at the Foreign Policy Research Institute and published author on asymmetric threats, presents another interpretation of asymmetry, labeled “Blank’s Theory.”²⁶ This classifies asymmetric threats within five dimensions:

1. they are threats of non-conventional nature;
2. they are designed to mislead the opponent;
3. they can be used by both state and non-state actors;
4. they do not imply confrontation, and;
5. they reflect the opponent’s strategy²⁷.

²⁴ Brittany Beaulieu and David Salvo. “NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence”. *Alliance for Securing Democracy*, no. 031 (June 2018): 1–7.

²⁵ Milica Ćurčić. “Asymmetric Threats”, 24.

²⁶ “Stephen Blank”. Foreign Policy Research Institute, April 24, 2020. Accessed August 24, 2020. <https://www.fpri.org/contributor/stephen-blank/>.

²⁷ Iskren Ivanov, Velizar Shalamanov. “NATO and Partner Countries Cooperation in Counter-Intelligence Asymmetric and Hybrid Threats in South Eastern Europe’s Cyberspace”. *Towards Effective Cyber Defense in Accordance with the Rules of Law* 149 (2020): 59–70.

In both scenarios, these tactics are intangible and entirely flexible, creating military action that is unpredictable, irregular, and difficult to combat.

Definitions: Hybrid Warfare

Hybrid warfare exists in concert with asymmetric threats, blending conventional and irregular tactics²⁸. In this sense, **hybrid warfare combines military and non-military as well as covert and overt means, fusing conventional capabilities with less-conventional ones** such as terrorist acts and criminal activities²⁹. Franck Hoffman, a Distinguished Research Fellow with the Institute for National Strategic Studies³⁰, builds from this definition: hybrid warfare incorporates different modes of warfare (both conventional and asymmetric capabilities), therefore utilizing synergistic efforts that are simultaneous, fused, and subordinated to one command unit³¹.

According to some military experts, this unconventional theatre of conflict can further be described as the “**Gray Zone**” of warfare, characterized by *“intense political, economic, informational and military competition more fervent than steady-state diplomacy, yet short of conventional war”*³², while employing *small-footprint, low-visibility operations often of a covert or clandestine nature*³³. This hybrid zone utilizes operations below internationally recognized thresholds and conventional, on-the-ground tactics. Though hybrid tactics are traditionally linked to non-state actors (terrorist organizations, for example) waging wars against more powerful foes,

²⁸ Brittany Beaulieu, David Salvo. “NATO and Asymmetric Threats”, 2.

²⁹ Laura-Maria Herta. “Hybrid Warfare – A Form of Asymmetric Conflict”. *International conference KNOWLEDGE-BASED ORGANIZATION* 23, no. 1 (July 20, 2017): 135–43. <https://doi.org/10.1515/kbo-2017-0021>.

³⁰ “Frank G. Hoffman”. Foreign Policy Research Institute, May 7, 2020. <https://www.fpri.org/contributor/frank-hoffman/>.

³¹ Laura-Maria Herta. “Hybrid Warfare”, 138.

³² Charles T. Cleveland, Charles T. Connett, Will Irwin, Joseph L. Votel,. “Unconventional Warfare in the Gray Zone”. Joint Force Quarterly. National Defense University Press, January 1, 2016. <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/>.

³³ Ibid.

Hoffman argues that hybrid wars do not supplant conventional warfare nor relegate future threats to sub-state actors³⁴. To this point, the Russian annexation of Crimea in 2014 and subsequent cyberattacks, media manipulation, and criminal agitation have been increasingly cited by policy experts (and contested by many others) as a prominent nation-state fusing conventional and asymmetric means under one command³⁵. Additionally, operating in the Gray Zone, the United States countered the September 11th terrorist attacks with small special operation forces (SOF), carrier and land-based airstrikes, and indigenous Afghan fighters to depose the illegitimate Taliban government giving refuge to al-Qaeda³⁶. Alongside their asymmetric means, the U.S. “boots on the ground” presence of roughly 350 SOF and other operatives made this a hybrid approach³⁷. Either state or non-state, consensus acknowledges hybrid warfare’s combination of tactics utilized, some conventional and some asymmetric, and the strategically and simultaneously coordinated efforts unlike wars of the past³⁸.

The History of Conventional Warfare

At the beginning of the 21st century, **conventional warfare** was loosely defined as the *confrontation of two or more countries to defeat the other through the use of armed forces*³⁹. More specifically, conventional warfare can be examined as *military action supported by economic pressure, information relations, and diplomacy from the state*. Through conventional political channels the government guides operations, the population provides the productive means, and the military uses them in conflict⁴⁰.

³⁴ Laura-Maria Herta, “Hybrid Warfare”, 138.

³⁵ Ibid, 135.

³⁶ Charles T. Cleveland, et al. “Unconventional Warfare”.

³⁷ Ibid.

³⁸ Ahmed Salah Hashim. “State and Non-State Hybrid Warfare”. Oxford Research Group, May 21, 2018. <https://www.oxfordresearchgroup.org.uk/blog/state-and-non-state-hybrid-warfare>.

³⁹ Huseyin Kuru. “Evolution of War and Cyber-Attacks in the Concept of Conventional Warfare”. *Journal of Learning and Teaching in Digital Age*, 2018, 12–20.

⁴⁰ Nikola Brzica. “Understanding Contemporary Asymmetric Threats”, 39.

This strategy has largely defined historical warfare. In 1945, United States forces, under the command of General Douglas MacArthur, approached Manila, the capital of the Philippines, in an attempt to eradicate Japanese presence from the island⁴¹. Japanese forces intended to defend the city, and in the face of tremendous ground casualties, American air commanders persisted in requesting General MacArthur to approve aerial bombardment to assist U.S. ground troops. MacArthur repeatedly denied the request, stating that while Japanese forces would likely be killed, so too would innocent Filipino civilians⁴². Without aerial support, both sides suffered heavy casualties, though the United States prevailed in capturing the city. Nonetheless, as MacArthur argued, the world would have reacted in horror had the U.S. employed aerial forces⁴³. Circumventing the principles of conventional warfare was an unacceptable cost.

The complex history of conflict provides context for this reluctance to engage in any tactics deemed “irregular.” Constructed in academic literature, the classification of warfare strategy divides warfare into four “generations”, (five phases)⁴⁴. Each generation features radically different warfare strategy: tactics conveyed in Manila have few parallels to methods embraced by the Greeks or modern Iraqi fighters. The generations include:

1. Wars before nation-states;
2. “Classical Warfare” (Generation 1), including the Napoleon wars and embracing lined arrangements of musketmen on battlefields;
3. “All Together Industry” (Generation 2), including World War I as the industrial revolution and wider railroad availability ushered in auxiliary and infantry units;
4. “Maneuver Wars” (Generation 3), extending back to WWII and embracing “blitzkrieg” strategies targeting the weakest part of an enemy;
5. “Unconventional Wars” (Generation 4), including the aftermath of September 11th and the Iraq and Afghanistan occupations⁴⁵.

⁴¹ William J. Fenrick. “The Rule of Proportionality and Protocol in Conventional Warfare”. *Hein Online*, 1982, 91.

⁴² *Ibid*, 91.

⁴³ *Ibid*, 91.

⁴⁴ Huseyin Kuru. “Evolution of War”, 13.

⁴⁵ *Ibid*, 13.

Evident above, the fourth generation departs quite extremely from prior wars and encompasses asymmetric and hybrid methods unique to modern conflict. A 1989 article in the Marine Corps Gazette (a professional journal for the US Marines disseminating military art and science)⁴⁶ introduced the concept of “**fourth generation warfare**” as *warfare that is widely dispersed and undefined, a vanishing distinction between war and peace, non-linear to the point of no definable fronts, and losing the distinction between “civilian” and “soldier.”*⁴⁷ This centers on the ability of weaker powers to combine conventional and irregular tactics to pose a legitimate threat to an opponent’s political will. As such, the fourth generation (constituting hybrid warfare) does not attempt to win by defeating an enemy’s military forces, but through hybrid tactics aimed at an enemy’s political will⁴⁸.

Warfare's Transition

As warfare progresses, the question remains: why are asymmetric and hybrid strategies dominating global conflict? Curiously, the answer lies in defensive efforts against these tactics: extreme discrepancies between actors’ military capabilities has incentivized the use of asymmetric and hybrid threats⁴⁹. In other words, there is a disparity between actors with the capacity to accumulate large armies, and those without. This has created an environment where less powerful actors must engage in hybrid tactics to eradicate inequality⁵⁰. The U.S. and its allies best represent this, with their national budgets constituting 40% and roughly a third of global spending⁵¹. “Weaker” nation-states, which qualifies nearly the entire world in comparison, cannot compete through conventional channels with the west. Thus, historical wars pitting two nations against each other on a battlefield have been rendered obsolete.

⁴⁶ “Marine Corps Gazette”. Marine Corps Gazette | Small Wars Journal. Accessed August 24, 2020. <https://smallwarsjournal.com/author/marine-corps-gazette>.

⁴⁷ Herta, Laura-Maria. “Hybrid Warfare”, 137.

⁴⁸ Ibid, 137.

⁴⁹ Huseyin Kuru. “Evolution of War”, 14.

⁵⁰ Ibid, 14.

⁵¹ James N. Miller and Michael O’Hanlon. “Quality over Quantity”, 2.

Inequality in military capacity is not the lone transforming force: **the doctrine of mutually assured destruction (MAD)** is an *evolutionary defense policy based on the logic that neither the United States nor its adversaries would start a nuclear war as the other would retaliate massively, with nuclear weapons potentially destroying the entire world*⁵². This doctrine applies narrowly to nations of nuclear capacity, yet serves as an additional deterrent to conventional war. In sum, post-Cold War society has forced non-state and nation-state actors to pursue irregular tactics in warfare to combat an escalating arms race between opposing ideological blocs. These conditions are directly responsible for the transition away from conventional warfare, and their maintenance on a global scale will only serve as additional encouragement of the usage of asymmetric threats and hybrid tactics.

Though conventional war has seen a decline in modern conflict, it remains in use for global powers against weaker nations and vice versa. Demonstrated by trends outlined above, this type of warfare is becoming difficult, outdated, and ineffective. Nonetheless, especially alongside hybrid tactics, conventional warfare can be advantageous. The U.S. government has engaged in aspects of conventional warfare against the Ba'ath Party government in Iraq⁵³. This nation-state against nation-state, enemy-specific attack was replicated to an extent in Crimea in 2014, where Russian troops invaded the peninsula and combined hybrid with conventional tactics⁵⁴. These examples demonstrate increasing hybrid tactics, but also the need for nations to remain vigilant against conventional ones.

Actors of Warfare

From the perspective of conflict analysis, **actors** in warfare are *all those engaged in or being affected by conflict*, otherwise considered “who

⁵² Alan J. Parrington. “Mutually Assured Destruction Revisited”. *Airpower Journal*, 1997, 4–19.

⁵³ David L. Buffaloe. “Defining Asymmetric Warfare”. Association of the United States Army, November 15, 2017. <https://www.ausa.org/publications/defining-asymmetric-warfare>.

⁵⁴ Taras Kuzio and Paul D'Anieri. “Annexation and Hybrid Warfare in Crimea and Eastern Ukraine”. E-International Relations, July 5, 2018. <https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/>.

intervenes"⁵⁵. John McDonald, a former U.S. Ambassador, diplomat, and peacebuilding expert⁵⁶, introduced the concept of "Multi-Track Diplomacy" which distinguished nine tracks of actors. From this, two significant sub-groups emerged: "states/governments" and "non-state actors", with several broad categories stemming below each⁵⁷. For the purpose of this paper, actors will refer to these large sub-groups, characterizing each actor as being tied (or not being tied) to a sovereign nation, therefore as "state", or "non-state." Though state actors are capable (and willing) to organize asymmetric efforts, their position on asymmetric conflict generally opposes non-state's and therefore are considered separately.

The **state** contains traditional military and political authority which relies on its own economic and diplomatic power⁵⁸. Comparatively, **non-state actors** employ a non-hierarchical structure of motivated "cells" with common motivations and political goals⁵⁹. This compartmentalization works in favor of organizations such as terrorist groups that must leave potential vulnerabilities decentralized. These actors are inherently different, crucially so in regards to sovereignty: according to a report released by the National Intelligence Council, non-state actors are non-sovereign entities and therefore are not legitimized on a global stage⁶⁰. Nonetheless, comprehension of both actors is vital to discussion surrounding asymmetric and hybrid warfare. Russia, a powerful nation-state, and the Islamic State, a terrorist non-state actor, operate vastly differently despite both engaging in hybrid and asymmetric tactics, and both must be understood in prospective defensive efforts.

⁵⁵ "Actors and Tactics of Conflict Interventions (Civilian Intervention and Nonviolent Intervention)". Irénées: A Website of Resources for Peace. Accessed August 25, 2020. http://www.irenees.net/bdf_fiche-analyse-659_en.html.

⁵⁶ "In Memoriam: Ambassador John W. McDonald". United States Institute of Peace, May 30, 2019. <https://www.usip.org/press/2019/05/memoriam-ambassador-john-w-mcdonald>.

⁵⁷ "Actors and Tactics" Irénées.

⁵⁸ Nikola Brzica. "Understanding Contemporary Asymmetric Threats", 41.

⁵⁹ Ibid, 41.

⁶⁰ "Non-State Actors: Impact on International Relations and Implications for the United States". National Intelligence Council. National Intelligence Officer for Economics and Global Issues, August 23, 2007. https://www.dni.gov/files/documents/nonstate_actors_2007.pdf.

State Actors

State-actors represent the traditional consolidation of authority and the central elements of the international system⁶¹. A **state** is defined as *a politically organized body of people at an established territory with public authority and the legal use of force and violence*⁶². This monopoly on violence differentiates sovereign states from other actors that lack similar territory or authority⁶³. Importantly, nations must be recognized by other sovereign states through international channels, such as the United Nations, to achieve this status. Further, the state must have public authority, governing tools, and territory and population to rule⁶⁴. Legality aside, certain states exercise conflict beyond their borders, wielding armies large enough to warrant conventional conflict or relying on hybrid and asymmetric means to circumvent international laws that would inflict potential consequences.

State Actors: Libya and Russia

Nation-states are capable of abusing asymmetric tactics to achieve political goals, as exemplified by the Libyan Civil War between the internationally recognized Government of National Accord and the Libyan national Army⁶⁵. Neighboring nations and global powers have become increasingly involved through asymmetric tactics. For example, both Turkey and Russia have trained mercenaries to be dispatched in Libya⁶⁶. Elsewhere, Turkey and the UAE have continued devastating airstrikes, jockeying over (what

⁶¹ "State Actors – Actors in International Relations". Coursera. International Relations Theory. Accessed August 16, 2020. <https://www.coursera.org/lecture/international-relations-theory/state-actors-0GRQe>.

⁶² Ibid.

⁶³ Ibid.

⁶⁴ Ibid.

⁶⁵ Nathan Vest and Colin P. Clarke. "Is the Conflict in Libya a Preview of the Future of Warfare?" Defense One. Defense One, June 2, 2020. <https://www.defenseone.com/ideas/2020/06/conflict-libya-preview-future-warfare/165807/>.

⁶⁶ Ibid.

some consider) the largest drone war in the world⁶⁷. Disinformation campaigns have increased alongside physical strikes, particularly through bots and trolls in favor of the Libyan national Army deployed by Russia, the UAE, and Saudi Arabia⁶⁸. These developments demonstrate modern “wars at distance”: technology, social media, proxy wars, and private armies of mercenaries allow states to participate in conflict and destabilize opposing governments without actively engaging in the carnage.

Whereas the Libyan conflict featured nation-states and non-state actors in coordination, Russia’s aggressive international actions have demonstrated the capability for a state to execute hybrid and asymmetric attacks without international assistance and without a pre-existing conflict. Through tactics of disinformation, cyberwarfare, and support for foreign political movements, Russia has tactfully played the line below conventional war⁶⁹. In 2017, a disinformation campaign (widely believed to originate in Russia) falsely accused German soldiers deployed in Lithuania of raping a teenage girl, stirring anti-soldier sentiments⁷⁰. Elsewhere, Russian disinformation efforts have targeted North Atlantic Treaty Organization (a political and military alliance seeking freedom and security for its members, shortened as NATO)⁷¹ partner countries to undermine citizen’s support for joining the alliance, in addition to cyberattacks targeting the Democratic National Convention in the United States, leaking vulnerable information online that jeopardized U.S election security⁷². In these scenarios, Russian efforts sought destabilization, manipulation of citizens, and vulnerability in nations Russia considers as global foes. This is evident further in Russian overt and covert support for political groups, funding a French far-right national group and supporting networks of non-governmental organizations shifting European public opinion towards a positive view of Russian politics⁷³.

⁶⁷ Ibid.

⁶⁸ Ibid.

⁶⁹ Brittany Beaulieu and David Salvo. “NATO and Asymmetric Threats”, 2.

⁷⁰ Ibid, 3.

⁷¹ “NATO / OTAN”. What is NATO? North Atlantic Treaty Organization. Accessed August 25, 2020. <https://www.nato.int/nato-welcome/index.html>.

⁷² Brittany Beaulieu and David Salvo. “NATO and Asymmetric Threats”, 3.

⁷³ Ibid, 3.

Russia is just one example of a prominent nation-state engaging in hybrid tactics. Both in states with the capabilities for conventional warfare and those who fight proxy wars abroad, asymmetric threats have proven effective in causing mass disruption to national governments and supra-national organizations. Thus, as their effectiveness remains consistent on a global stage and their methods remain under the threshold for conventional war, defense strategies must be adjusted to fully combat asymmetric means and security experts must acknowledge the threat that nation-states pose.

Non-State Actors

Non-state actors are defined as *non-sovereign entities that exercise political, economic, or social control at either a national or international level*⁷⁴. These actors operate outside the confines of a conventional state, pursuing their political agendas through means more difficult to contain or regulate. Forming a consensus on non-state actors has proven difficult for scholars and national governments alike. Nonetheless, a flexible list includes the following, per the United States National Intelligence Council:

1. multinational corporations and organizations;
2. nongovernmental organizations (NGOs);
3. super-empowered individuals;
4. terrorist organizations;
5. criminal networks⁷⁵.

This is not a summative list, but rather an introduction to several non-state actors in global politics. However, in the context of hybrid warfare, terrorist organizations and criminal networks participate as the most important actors.

In examining conflict, two main groups of non-state actors can be identified in accordance with their operating tendencies. **Non-violent non-state actors**, including multinational corporations, *can have profound effects on a nation's economic or political state, with the potential to also exert*

⁷⁴ "Non-State Actors" National Intelligence Council.

⁷⁵ "Non-State Actors" National Intelligence Council.

*harmful influence or undue control over a region*⁷⁶. **Violent non-state actors**, however, generally *present national and international consequences of extreme magnitude, and are characterized by their ability to rely on violence and force through asymmetrical channels*⁷⁷. Inclusion as a violent non-state actor ranges from militias and warlords, to terrorist and criminal gangs, and insurgents and transnational criminal groups⁷⁸. As previously theorized, the usage of asymmetric and hybrid threats stems from a disadvantaged military position, where non-state actors or weaker states must approach warfare through irregular and unexpected tactics to sustain victory. This becomes evident when examining specific examples of non-state actors and their methods, such as terrorist organizations operating in the Middle East, Africa, or South East Asia.

Non-State Actors: Terrorist Organizations

On September 11th, 2001, the actualization of asymmetric threats posed by non-state actors was realized. Hijacking commercial aircrafts and piloting them towards buildings symbolizing the global authority of the U.S. departed quite extremely from warfare in the trenches, and this shifted U.S. foreign policy to the primary role of counterterrorism⁷⁹. The administration of President George W. Bush declared a “War on Terror”, gathering information and targeting the terrorist non-state actors responsible, which represented the United States’ own effort in hybrid warfare and dealing with non-state actors⁸⁰. U.S. forces operated in the previously defined

⁷⁶ Ibid.

⁷⁷ Ibid.

⁷⁸ Thomas Risse, Tanja A. Börzel and Anke Draude. *The Oxford Handbook of Governance and Limited Statehood*, 2018.

⁷⁹ Anthony H. Cordesman. “The Lessons and Challenges of September 2011 – the New ‘9/11.’” *The Lessons and Challenges of September 2011 – the New “9/11”* | Center for Strategic and International Studies. Center for Strategic and International Studies, August 14, 2020. <https://www.csis.org/analysis/lessons-and-challenges-september-2011-%E2%80%93-new-911>.

⁸⁰ Anthony H. Cordesman. “The Lessons and Challenges of September 2011 – the New ‘9/11.’” *The Lessons and Challenges of September 2011 – the New “9/11”* | Center for Strategic and International Studies. Center for Strategic and International Studies, August 14, 2020. <https://www.csis.org/analysis/lessons-and-challenges-september-2011-%E2%80%93-new-911>.

“Gray Zone”, deploying special operation forces (SOF), carrier and land-based airstrikes, and irregular Afghan fighters to depose the illegitimate Taliban government giving refuge to al-Qaeda⁸¹.

Despite fighting occurring largely in nation-states of Iraq and Afghanistan, the perceived threats from U.S. strategy were al-Qaeda and the Taliban, emphasizing the role that non-state actors can play in global conflict and their complicated relationship with nation-states⁸².

The September 11th terrorist attacks and subsequent geopolitical consequences modeled an increasing fusion of non-state and state forces. This created a gap in contemporary military terminology and strategy, filled today by the widely utilized “asymmetric and hybrid threats”⁸³. Neither terrorism, the organizations behind these attacks, nor the following U.S. invasion were “new concepts” in 2001. However, combining conventional “on the ground” military action (such as the deployment of U.S. SOFs) with irregular methods of insurgency, war on information, and cyberattacks represented a departure from previous military strategy⁸⁴. Further, despite frequent terrorist activity both prior to and since September 11th, this awoke much of the world to potential threats posed by terrorist (and generally non-state) actors such as al-Qaeda, and presently the Islamic State.

Platforms of Warfare

After the dramatic arrival of asymmetric threats in global conflict, national defense strategies eagerly rushed to identify and address potential tactics. This proclivity ran counter to an actual comprehension of the term: asymmetry quickly came to define every threat faced in international conflict and this careless application rendered the concept useless⁸⁵. Substantive critique from academics contested the label of threats themselves as

⁸¹ Charles T. Cleveland, et al. “Unconventional Warfare”.

⁸² Anthony H. Cordesman. “The Lessons and Challenges”.

⁸³ Milica Ćurčić. “Asymmetric Threats in Security Studies”. 23.

⁸⁴ David L. Buffaloe, “Defining Asymmetric Warfare”.

⁸⁵ Stephen J. Blank, *Rethinking Asymmetric Threats*. Commonwealth Institute, 2003.

asymmetric, instead of the nature of strategies utilized⁸⁶. In reference to “platforms” of asymmetric and hybrid warfare, this paper seeks to identify and address this complaint.

The idea of “platforms of warfare” is not widely addressed in academia, and this makes asymmetric tactics difficult to reliably quantify. Therefore, this paper seeks to introduce the concept of **platforms of warfare** as *an overarching classification of asymmetric threats characterized by the nature of the threat utilized*. This definition relies on the logic that asymmetric and hybrid tactics, or “means” exist within a greater conceptual platform. For example, a cyberattack is an asymmetric threat dependent on computer technology and communication networks. From this, cyberattacks can be determined to exist within the platform of information warfare.

Beyond this, this paper acknowledges a platform widely utilized today and referenced above: information warfare. This example is not an all-encompassing list; several other platforms exist, notably terrorist activity. To maintain the scope of this paper, however, information warfare will be briefly explored while cyberattacks, a central asymmetric threat within that platform, will receive an in-depth case study.

Platforms: Information Warfare

The past few decades have revolutionized information and communication technologies in society, introducing modern telephones, radio signals, and satellites. To optimize military strategy, warfare has shifted alongside technology: broadly, **information warfare** is *a struggle over these information and communication systems, and the application of destructive force on a large scale against information assets and systems and against the computers and networks that support this critical infrastructure*⁸⁷. These increased communication systems have created a societal reliance on them, leaving organizations potentially vulnerable

⁸⁶ Ibid.

⁸⁷ Brian C. Lewis, “Information Warfare”. *Federation of American Scientists*, Accessed August 17, 2020. <https://fas.org/irp/eprint/snyder/infowarfare.htm>

to information warfare damaging or freezing their networks. However, increased communication systems can be similarly favorable to offensive information attacks: whereas once information was a tool of the state, (in certain nations it remains that way) asymmetric opponents today wield the power to make and distribute their own information to much wider audiences⁸⁸. This ability has ushered in new areas of conflict operation, enabled states to engage in mass disinformation campaigns, and allowed wars to be fought remotely behind a monitor⁸⁹.

Commonly utilized by rogue nations or non-state actors seeking destabilization, cyberattacks and cyberwarfare are central to information warfare. These tactics represent a particularly advantageous strategy due to the limited assets they require: with secure networks and infrastructure, actors can leverage massive disruption and destabilize government networks, elections, or the networks of supranational organizations from abroad⁹⁰. This capability of “warfare from abroad” allows states to conceal their actions or motives, avoid international consequences (such as sanctions) or prevent the carnage possible in conventional intervention.

During the Kosovo War in 1999, Serbian hackers, in concert with their Eastern European sympathizers, launched global attacks aimed at shutting down key computer systems in NATO countries⁹¹. Despite knowledge that this attack was not sufficient to win the war, the Serbs successfully stalled the NATO offensive and disabled temporary response and communication systems⁹². These cyberattacks are rudimentary compared to information warfare of today: among other nation-states and non-state actors, China and Russia are capable of waging catastrophic cyberattacks

⁸⁸ Rod Thornton, *Asymmetric Warfare: Threat and Response in the 21st Century*. Polity Press, 2007.

⁸⁹ Ibid, 62.

⁹⁰ Ray Song. Publication. *The Hermit Threat: A Historical Analysis of Cyberwarfare, Its Modern Manifestations in North Korea, and Its Implications in Global Relations of the 21st Century*, 2017.

⁹¹ Rod Thornton. *Asymmetric Warfare*, 62.

⁹² Ibid, 62.

on rival states, vastly more damaging than those utilized by Serbia in 1999. With disinformation campaigns, trained cyber experts, and the world's increasing reliance on global networks, these powers have many vulnerable targets to exploit and will continue to do so under the threshold of warfare.

As mentioned previously, information warfare is not the lone platform of asymmetric means. Though broad in scope, terrorism represents another. This includes attacks leveraged by terrorist organization, though terrorism may also result from state-waged violence through the use of weapons of mass destruction, biological weapons, attacks on critical infrastructures that society depends on, or from attacks on people and institutions of the federal government⁹³. The threat of terrorism continues to loom large over the western world especially as military accumulation forces non-state actors to utilize irregular tactics. Therefore, this platform must be addressed as fervently as information warfare in an effort to stall its global rise.

Asymmetric Threat Case Study: Cyber Attacks

Cyber operations and their role in conflict represent a dramatic shift in society over the past few decades. Under the veil of anonymity and the threshold for conventional conflict, cyberattacks are an emerging asymmetric threat being utilized to create great destruction. Academia hosts several definitions for the concept of **cyberattacks**, though specifically for this paper they refer to *"...hostile acts using computer or related networks to disrupt or destroy an adversary's cyber systems or functions."*⁹⁴. Whereas cyberattacks refer to isolated incidents, **cyberwarfare** expands upon this concept as *"...massively coordinated digital assaults on one government by another or by large groups of citizens, as when cyber attacks are orchestrated by state-sponsored hackers against another nation's cyber*

⁹³ Ashton B. Carter, William J. Perry, and David Aidekman. "Countering Asymmetric Threats". Belfer Center, n.d., 1–10.

⁹⁴ Ray Song. *The Hermit Threat*, 2.

infrastructure."⁹⁵. Examining these concepts, there are generally three targets of cyberwarfare:

1. information itself;
2. information processes that disseminate and analyze material of the state;
3. the infrastructure of information systems that store, transmit and process said material⁹⁶.

The utilization of cyber methods against these targets offer actors operational flexibility, convenience, and undue authority. Computer attacks can be launched remotely or anonymously so as to avoid direct consequence, while their non-physical existence offers less-able nation-states to be equally disruptive as their more-powerful counterparts⁹⁷. Whereas traditional warfare required a level of capability to launch an attack, cyber methods have created a sphere of conflict where power can be utilized by a wide array of political instigators for damaging purposes⁹⁸. From this, defending national security systems proves difficult, especially considering how many potential threats exist: terrorist organizations, disgruntled individuals, or even hostile nation states can overpower cyber systems manned by limited numbers.

In recent decades, Russia has utilized cyber attacks as a means of promoting their political agenda abroad. In some instances, these tactics combined with conventional conflict in the form of hybrid warfare. In 2007, following a dispute between the Estonian and Russian national governments, pro-Kremlin forces froze Estonian networks⁹⁹. Not officially state-run, these attacks were orchestrated by non-state actors and asymmetric in quality¹⁰⁰. The following year amidst the Russo-Georgian War, Russian

⁹⁵ Ibid., 3.

⁹⁶ "Information Warfare: Cyber Warfare Is the Future Warfare". *Global Information Assurance Certification Paper*, 2004.

⁹⁷ Ray Song. *The Hermit Threat*, 2.

⁹⁸ Ibid., 2.

⁹⁹ Ibid., 6.

¹⁰⁰ Ibid., 6.

criminal gangs attacked multiple Georgian government targets, marking the first time that a known cyber attack had coincided with shooting in war¹⁰¹. This utilization of asymmetric means alongside conventional strategy explicitly demonstrates hybrid warfare.

North Korea is an additional proponent of cyber attacks. Lacking strategic advantages of large enlistment numbers, foreign investments, and advanced technical equipment, North Korea uses asymmetric strategies to offset warfare disparities against more powerful opponents¹⁰². This has made cyber attacks a strong strategy for North Korea: cyber attacks can be conducted from abroad, require limited assets, and relies on little manpower to wreak considerable havoc abroad. Further, North Korea leverages their detachment from global cyber networks to manipulate cyber attacks as a viable strategy¹⁰³.

Recognizing their reliance on cyber attacks, the North Korean national government has made considerable efforts to funnel their brightest students into computer hacking and cyberwarfare operations¹⁰⁴. Government officials select promising students in mathematics to learn computer-based warfare. These students are then trained in specialized organizations before entering computer hacking forces, the most prestigious known as Bureau 121¹⁰⁵. Forces like these have been successful in enabling North Korea to engage in asymmetric combat from a distance, in soliciting funds for national use, and in incapacitating enemies of their ideology¹⁰⁶.

In February of 2016, \$101 million dollars was taken from a New York Federal Reserve account that belonged to a Bangladesh Central Bank¹⁰⁷. A single spelling error on a withdrawal request raised the alarm that prevented the

¹⁰¹ Ibid., 6.

¹⁰² Ibid., 8.

¹⁰³ Ibid., 8.

¹⁰⁴ Ibid., 9.

¹⁰⁵ Ray Song, *The Hermit Threat*, 9.

¹⁰⁶ Ibid., 9.

¹⁰⁷ Ibid., 10.

initial request of \$1 billion from being authorized¹⁰⁸. This attack, discovered to have occurred in banks in over ten other nations, was eventually signaled to have come from North Korea. However, due to a lack of physical evidence, the funds were never recovered and are potentially in circulation in North Korea markets¹⁰⁹. This attack demonstrates the sheer capabilities of cyber attacks and the flexibility in their use. Rogue nation-states or non-state actors wield the capability to freeze networks, shut down entire governments, or steal significant sums of money, all without direct conflict, under the threshold of warfare, and without global repercussions.

Responses to Asymmetric and Hybrid Threats

Modern conflict's shift to asymmetric and hybrid tactics represents one of the most pressing matters in global security. Following the arrival of these tactics on the international stage, defense doctrines and recommendations were released by national and supra-national governing bodies to outline methods of prevention. These responses were preliminary in nature and are continually evaluated to properly address evolving threats. For example, increasing Russian hybrid activity has alarmed nations in Europe and NATO into further hybrid warfare prevention¹¹⁰. As these issues continue to disrupt global processes, effective responses become increasingly crucial for international security and must comprehensively address and alleviate threats posed by asymmetric tactics.

In addressing responses to asymmetric and hybrid threats, this paper will outline current European procedure. Though response strategies to these threats will vary depending on the nature of conflict to specific regions, European alliances, specifically NATO, have formulated comparatively advanced response systems that will be discussed as models for other global regions to utilize. These responses may not apply uniformly, especially considering NATO's status as a supra-national organization.

¹⁰⁸ Ibid., 10.

¹⁰⁹ Ibid., 11.

¹¹⁰ Brittany Beaulieu and David Salvo. "NATO and Asymmetric Threats", 2–3.

Nonetheless, the principles that they rely on are crucial to combating asymmetric threats on a global level.

NATO's Response Strategy

At the 2008 Bucharest Summit, NATO presented their Comprehensive Approach Action Plan, a framework for the mobilization of military and civilian resources to resist hybrid challenges¹¹¹. This represented a crucial first step in acknowledging the threat of asymmetric and hybrid tactics, which to that point had not entered the public sphere. In December of 2015, this progress continued: NATO adopted a strategy of confronting hybrid threats by increased partnership with the European Union (EU). This partnership included information sharing between member states, warning signs of hybrid threats at the alliance's border, and encouraging members to recognize potential vulnerabilities within their own system to Russian interference¹¹².

In recent years, joint-defense efforts have been expanded by both EU and NATO officials. The two alliances have coordinated response strategies and established centers dedicated to the analysis and development of hybrid defense, among them the European Center of Excellence for Countering Hybrid Threats¹¹³. This coordination relays joint declarations and recommendations to member states, calls on individual national governments to identify internal weaknesses, and encourages members to contribute to a greater security threshold in Europe¹¹⁴. Despite these promising advancements, it remains true that NATO defense strategies are not being optimized and they face institutional challenges to success.

Though NATO and the EU have pledged cooperation in their war on asymmetry, their efforts remain stalled by a lack of funding, a lack of membership

¹¹¹ Ray Song, *The Hermit Threat*, 3.

¹¹² *Ibid.*, 3.

¹¹³ *Ibid.*, 4.

¹¹⁴ *Ibid.*, 3.

commitment, and information blocking¹¹⁵. Specifically, between the two organizations there exists no tool to share classified, high-level information crucial to alliance defense policy¹¹⁶. In situations of pressing hybrid challenges, this lack of information sharing across organizations ensures a less effective response. Attempts to promote information sharing within the organizations has proved challenging. For example, despite Russian cyber and disinformation attacks on the U.S. 2016 election, the nation shared little information with fellow NATO members¹¹⁷. Fundamentally, this hesitance makes sense: even with allies, nations are skeptical of discussing internal vulnerabilities. Nonetheless, this approach to information sharing has stunted the alliance's ability to appropriately respond to hybrid threats and create uniform responses to urgent issues¹¹⁸.

Further, despite centers positioned to address asymmetric and hybrid threats, NATO's identification policy is unclear. In modern conflict, hybrid forces are commonly fused with conventional warfare and oftentimes exist without underlying conflict. Despite this common occurrence, NATO's internal framework addressing these conflict levels has no concrete response¹¹⁹. In addition, response strategies are stalled by NATO members' varying perceptions of threat regarding asymmetric tactics. Nation-states susceptible to Russian influence in Eastern Europe may call for increased protections against information warfare, while nation-states overwhelmed by migration from the Middle East in Southern Europe may wish to adjust focus to criminal activity. NATO must find a way to blend their response strategies to fit this range of issues, or else remain fractured and pulled along by their member's diverse interests. Ultimately, it proves difficult to organize an alliance on a single issue in the face of many.

¹¹⁵ Ibid., 4.

¹¹⁶ Ibid., 4.

¹¹⁷ Ibid., 4.

¹¹⁸ Ibid., 4.

¹¹⁹ Ibid., 4.

Recommendations to Asymmetric and Hybrid Threats

While malicious state and non-state actors continue to engage in asymmetric and hybrid tactics, other global actors must not be complicit in their progress and must recognize necessary procedures to be enacted. Proactively, this recognition must translate to policy and definite changes. Therefore, this paper will identify several recommendations to effectively challenge asymmetric tactics in modern society. As European responses to hybrid warfare were outlined above, a NATO-specific recommendation will be discussed. However, as recommendations are crucial to regions that do not already have functioning response systems to hybrid threats, generalized recommendation strategies will be additionally addressed.

NATO principally relies on their stated articles to govern and direct the alliance. These articles, meant to provide guidance in times of crises, are not being effectively enforced in unifying a defense strategy. NATO Article 4 states that parties (nation-states) will consult together when, in the opinion of any member, the political independence or security of a member is threatened¹²⁰. As previously mentioned, certain NATO members have not been transparent in their struggles with hybrid threats, particularly when it exposes vulnerabilities in a nation's infrastructure or defense capabilities. Nonetheless, the alliance must invoke article 4 to enable these difficult consultations and to properly address areas in alliance security where foreign actors may be meddling. To respond effectively, individual nations should develop internal thresholds that identify asymmetric threats¹²¹. When crossed, this should serve as an alarm to bring the issue to the awareness of other NATO members. Then, NATO should facilitate consultations that organize effective responses to hybrid operations. In doing so, a NATO-wide response team to assist member-states struggling with conflict would be incredibly constructive for the alliance going forward¹²².

¹²⁰ NATO. "The North Atlantic Treaty". NATO. North Atlantic Treaty Organization, April 1, 2009. https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

¹²¹ Brittany Beaulieu and David Salvo. "NATO and Asymmetric Threats", 5.

¹²² Ibid., 5.

Elsewhere in the world, especially in regions plagued by terroristic activity or struggling with other governmental-infrastructure, responses to hybrid and asymmetric threats are crucial in securing national defense. These recommendations are not nation or alliance-specific, but rather they represent actions that would be beneficial outside the scope of an international organization or any individual nation-state.

For an effective national response to asymmetric threats, response mechanisms must be institutionalized. There is no universal solution to asymmetric threats; even among related means, such as chemical and biological warfare, responses differ greatly and can complicate defense strategies¹²³. Therefore, responses must be institutionalized by the national military and governing bodies: in doing so, doctrine, strategy, structure of armed forces, and training must be addressed in policy and procedure to ensure a timely and effective response to hybrid attacks¹²⁴. Further, understanding that variable asymmetric means warrant varying responses, an integrated and institutionalized defense effort should incorporate two primary efforts: protection and threat management¹²⁵. In other words, though each unique type of asymmetric attack calls for its own individualized response, a national system must be organized with responses categorized by defensive protections versus proactive threat management. Defensively, this would establish procedures in the scenario of an incoming or on-going asymmetric attack, whereas coordinating threat management systems would attempt to prevent any attacks from materializing¹²⁶. These efforts should be coordinated with allied states and national partners to standardize responses globally.

Specific to the African subcontinent, several additional recommendations will be made to secure nations from impending hybrid and asymmetric threats. Some of these threats are contingent on region-specific qualities, however the recommendations are applicable to a global audience.

¹²³ Bruce W. Bennett, "Responding to Asymmetric Threats", Essay. In *New Challenges, New Tools for Defense Decisionmaking*, RAND Corporation, n.d.

¹²⁴ Ibid., 50.

¹²⁵ Ibid., 50.

¹²⁶ Ibid., 50.

First, nations should revisit and revise their threat-response mechanisms¹²⁷. Threats often assume a transnational capacity, exposing weaknesses in the state. Therefore, existing institutions and defense approaches need to constantly adapt to emerging threats as they appear¹²⁸. In states that are particularly fragmented or with less centralized governments, this revision and policymaking process should include the involvement of local or religious leaders who would be most knowledgeable of the threats their community faces¹²⁹. Next, the coordination of efforts and existing strategies is imperative for a successful defense system. This revisits the issue of government fragmentation or decentralization: it is possible that within government bodies of a state, information sharing and communication procedures are ineffective. To improve response systems, this must be fixed: intelligence and information sharing should be streamlined to be efficient and effective in the face of emergency threats¹³⁰. As part of this information process, warning networks and response mechanisms should be established and optimized. However, these mechanisms will only alert the acting government of a potential threat. Following, there must be some state capacity to respond to or prevent said hybrid attack from progressing. This may be in the form of increased national intelligence organizations, increased staff of intelligence operatives and state-employees, stronger cyber infrastructure, or increased military capability to deter armed threats¹³¹.

As part of the necessity for state capacity, it is recommended that nations improve their infrastructure as a means of defense¹³². The lack of a self-sufficient economy or reliable infrastructure leaves states vulnerable to crises or attacks. For example, an attack of biological warfare might be more effective and spread more thoroughly in a state with inadequate health

¹²⁷ Kwesi Aning. "Confronting Hybrid Threats in Africa: Improving Multidimensional Responses". Essay. In *Future of African Peace Operations*, edited by Mustapha Abdallah, 20–37. The Nordic Africa Institute, 2016.

¹²⁸ Ibid., 30.

¹²⁹ Ibid., 31.

¹³⁰ Kwesi Aning. "Confronting Hybrid Threats in Africa: Improving Multidimensional Responses". Essay. In *Future of African Peace Operations*, edited by Mustapha Abdallah, 20–37. The Nordic Africa Institute, 2016, 31.

¹³¹ Ibid., 32.

¹³² Ibid., 32.

care¹³³. As a final recommendation, both for states defending against asymmetric threats and those that utilize them in conflict, the ability to resolve conflict without intervention, warfare methods, or illegal channels is important to global peace. International diplomacy, economic relations, and strategic policymaking must be more accessible and effective. For non-state actors and nations to abandon asymmetric means, there must be legal channels for their political agendas to be processed. This should exist through international organizations, alliances, and councils meant to support weaker states.

Conclusion

Asymmetric and hybrid threats represent the present and future of global warfare. The irregular nature of these threats allows them to adapt to opposing powers in conflict, making them especially effective on the international stage. As nation-states compete to accumulate arms and deter conventional attacks, less capable actors will continue to revert to asymmetric means to exercise their political aspirations. As such, nation-states and supra-national organizations such as NATO must establish and refine response systems to defend against these tactics. Utilizing the recommendations above, states should institutionalize their responses, streamline information-sharing procedures, and develop stable infrastructure to allow for increased state capacity. Most importantly, diplomatic means and resolutions must be developed beyond intervention or asymmetric means. The global security realm must not be complacent in their battle against asymmetric war and warfare's constant development. Otherwise, as states develop the capacity to defend against current methods of cyberattacks or terrorism, other means of warfare will arise to take their place.

¹³³ Ibid., 32.

Active Cyber Defense and Operational Environment Preparation: An Opportunity for Progress

Zoë BRAMMER

Abstract: The prevalence of threats in the cyber domain have become increasingly evident, as signaled by the widespread adoption of military strategies aimed directly at information flows in a race to establish “cyber dominance”. These strategies tend to be offensive in orientation, inefficient, and event-specific, causing them to rapidly become outdated. Due to the ever-changing nature of the cyber domain and the inability of a single state to dominate cyberspace, states should begin to adopt stronger defensive orientations in their quest for cybersecurity. This paper highlights two areas of cybersecurity—active cyber defense (ACD) and operational environment preparation (OEP)—that provide ample opportunity for cyber defense improvement. I then make three actionable recommendations, all of which address gaps in both ACD and cyber OEP that together will result in improved cybersecurity. In this way, improving cyber defense capabilities can be resource-efficient, sustainable, and effective.

Keywords: Cybersecurity, cyber defense, active cyber defense, cyber situational awareness, operational environment preparation

Introduction

The exponential speed at which the world has become more interconnected and interdependent is perhaps most directly evident in cyberspace. At the same time, threats originating from the cyber domain have accelerated in both number and sophistication. Such threats are transnational, highly contagious, and have the potential to completely halt the normal day-to-day operations of the international system, making them central to a state's security considerations. As a result, beginning in the first half of the 1990s, US strategic analyses "began to contain a growing number of warnings that national security was increasingly threatened by cyberattacks"¹³⁴, leading to the early formation of offensive strategies and doctrines aimed directly at information flows.

There is a fairly abundant body of literature on the emergence and containment of cyber threats, which can be boiled down into two main security considerations. First, many security scholars argue that a "major change in the security environment has occurred"¹³⁵. This is because cyber threats are "increasingly difficult, if not impossible, to peel away from the process of globalization"¹³⁶, and the increasing availability of and dependence on computers and the internet across the world. As a result, cyber threats cannot be easily contained. Unlike many security threats that arise in the four traditional military domains (land, sea, air, space), cyber threats "transcend the capacity of a single nation-state to confront them adequately"¹³⁷. Cybersecurity poses a new kind of security challenge to states across the globe and to the international community more broadly, and it requires the cooperation of the public, private, and international sectors.

¹³⁴ Myiam Dunn Cavelti. "The Politics of Cybersecurity: Balancing Different Roles of the State". *Center for Security Studies ETH Zurich*, 17 June 2019. css.ethz.ch/en/center/CSS-news/2019/06/the-politics-of-cybersecurity-balancing-different-roles-of-the-state-.html.

¹³⁵ Richard Sinnott. "Public Opinion and the New Security Environment". *European Union Institute for Security Studies (EUISS)*, 1997. N.p.

¹³⁶ Paul Rexton Kan et. al. "Lawyers, Guns, and Money: Transnational Threats and U.S. National Security". *Strategic Studies Institute, US Army War College*, 2010. 207.

¹³⁷ Ibid.

The second security consideration is that cybersecurity has become deeply integrated into all traditional military security domains as the military becomes increasingly reliant on cyber capabilities and conducts more operations within the cyber domain. The US military's global communications backbone, for example, "consists of 15,000 networks and 7 million computing devices across hundreds of installations in dozens of countries"¹³⁸. Over the past 10 years, the frequency and sophistication of intrusions into US military networks have increased exponentially¹³⁹, thereby threatening not only cyber operations but military operations in the traditional domains as well. As a result, cybersecurity is and will continue to be a central facet of military security more broadly.

Because the cyber domain exists mostly outside of the physical realm, cyber threats are unique in their propensity to move seamlessly between endangering "individual and collective security, between public authorities and private institutions, [and] between economic and political-military security"¹⁴⁰. Consequently, it is key to state security to establish effective cyber defense and prepare for offensive cyber operations. Unfortunately, traditional security operations and a large portion of general security studies literature have little to say about how best to prepare for and respond to cyber threats.

To date, the majority of cybersecurity considerations have been offensive in orientation, with the ultimate aim of establishing "cyber dominance". The premise of achieving cyber dominance is defined as a state that "achieves and maintains strategic and tactical dominance in its critical elements of cyberspace"¹⁴¹, but although a single state can own some of the computers and software in the cyber domain, it certainly cannot own

¹³⁸ William J. Lynn. "Defending a New Domain: The Pentagon's Cyberstrategy". *Foreign Affairs* 89, no. 5 2010. 98.

¹³⁹ *Ibid.*, 100.

¹⁴⁰ Lene Hansen and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School". *International Studies Quarterly* 53, no. 4 (2009): 1155–175. Accessed August 6, 2020. www.jstor.org/stable/27735139. 1161.

¹⁴¹ Martin R. Stytz., and Sheila B. Banks. "Toward Attaining Cyber Dominance". *Strategic Studies Quarterly* 8, no. 1. 2014. 55. www.jstor.org/stable/26270605.

a majority of them, and cyberspace itself, as a non-physical entity, cannot be owned by anyone. This is further complicated by the fact that the “vast majority”¹⁴² of critical cyber infrastructure and key resources are owned by the private sector (85 percent in the US¹⁴³, for example). In most states, there is a limit to how much control the government is willing to exert over the private sector’s decisions regarding cybersecurity. In the United States and the United Kingdom, for example, “the government regards privately owned and operated critical infrastructure as a key element of national security but is reluctant to claim a mandate to oversee network security. At the same time, the private sector is not inclined to accept responsibility or liability for national cyber security”¹⁴⁴. Because of the hesitation on the part of government to mandate that the private sector adopt stricter security measures, there is a temptation for cybersecurity to become offensive in nature, with states encouraging the development of offensive cyber capabilities without creating effective cyber defense measures. An offensive cyber orientation is appealing because it may require less cooperation between the public and private sectors and can give an illusion of control.

Adopting an offensive orientation towards cybersecurity is problematic however, because actors in cyberspace are extremely difficult to identify, especially in the wake of a cyber-attack (this is known as the attribution problem). The legal framework surrounding cyber warfare also remains unclear, making a cybersecurity approach based around offensive operations and retaliation less than ideal. Although cybersecurity has become “critical to...military operations”¹⁴⁵, the way we approach cybersecurity needs to be reassessed and reoriented towards defense.

At a very basic level, *strategic* cyber defense should aim to prevent penetration of *tactical* cyber defenses. Strategic cyber defense encompasses “*how*

¹⁴² Critical Infrastructure Sector Partnerships. 2019, April 23.

¹⁴³ Government Accountability Office, *The Department of Homeland Security’s (DHS) Critical Infrastructure Protection Cost-Benefit Report*, June 26, 2009. 1.

¹⁴⁴ Madeline Carr. “Public-private partnerships in national cyber-security strategies”. *International Affairs*. 43. <https://doi.org/10.1111/14682346.12504>.

¹⁴⁵ William J. Lynn. “*Defending a New Domain: The Pentagon’s Cyberstrategy*”. 101.

an organization defends itself and its overall cybersecurity posture”¹⁴⁶, and includes considerations of operational capacity. Tactical cyber defense considers “*what* an organization needs to focus on when responding to incidents”¹⁴⁷, and includes a discussion of technical cyber capabilities. If a cyber-attack penetrates a network system, tactical cyber defense should prevent the attacker from determining the cyber terrain and prevent the attacker’s malware from executing. In the event that malware does execute, strategic cyber defense should prevent the malware from accessing its target and/or communicating back to the attacker¹⁴⁸. Due to the rapidly evolving nature of the cyber domain, creating sustainable and effective cyber defense systems addressing each of these goals is extremely difficult. This paper aims to identify areas of cyber defense that should be the primary focus in developing cybersecurity both within individual states and in the international community more broadly.

Establishing defensive cybersecurity is a massive undertaking, and it is crucial that the pursuit of cyber defense capabilities take into account the realities of the existing limited resource base and the importance of not exposing the network to unnecessary vulnerabilities through the use of too many defense channels within critical networks. This paper develops a functional lexiconic framework for cybersecurity, describes two facets of cyber defense (active cyber defense and operational environment preparation) and identifies areas in which multiple defensive improvements can be accomplished using a single resource set.

Definitions

No study of cybersecurity can be useful without first providing a functional lexiconic framework. Given the fairly recent rise of cybersecurity and the

¹⁴⁶ Cyber Stratego: Strategic vs. Tactical Threat Intelligence. *ThreatConnect: Intelligence-Driven Security Operations*. September, 2016. Retrieved August 20, 2020, from <https://threatconnect.com/blog/strategic-vs-tactical-threat-intelligence/>.

¹⁴⁷ ThreatConnect, “Cyber Stratego”.

¹⁴⁸ Martin R. Stytz. et. al. “*Toward Attaining Cyber Dominance*”. 64.

cyber domain, many of the accompanying terms are not clearly defined. This is a major hindrance in establishing cybersecurity because it prevents actors from working in concert. Without the strong base of a common lexiconic framework, it is difficult for actors to define issues, let alone work together to solve them. Effectiveness depends on establishing a common terminology for the domain, the actors within the domain, and the threats that come from combining the two. Thus, to achieve operational efficiency, the following definitions should be applied in the staging of active cyber defense and cyber operational environment preparation.

Cyber Relevant Time

Although this definition is slightly dated (originally published in 2014), Herring neatly sums up the vagaries associated with cyber relevant time. Cyber relevant time is a “purposely vague term that accommodates the needs of the battle space”¹⁴⁹. If the battle space is between two computers of close physical proximity, for example, cyber relevant time is milliseconds to seconds. For a battlespace between two computers on opposite sides of the world via satellite links, cyber-relevant time is seconds. With live operators and delays inherent in cognitive processing, keystrokes, and mouse clicks, cyber relevant time is seconds to minutes¹⁵⁰. The term simply implies that in different contexts, the speed at which systems operate is different, and the requirements for the speed of effective defense differs as well.

Traditional Military Domains

The four traditional military domains are sea, land, air, and space. They are considered traditional in that for the most part, definitions of security within these domains revolve around physical characteristics like geographical locations or physical equipment.

¹⁴⁹ MJ Herring and KD Willett. “Active Cyber Defense: A Vision for Real-Time Cyber Defense”. *Journal of Information Warfare* 13, no. 2 (2014): 46–55. Accessed July 31, 2020. www.jstor.org/stable/26487121.

¹⁵⁰ *Ibid.*, 47.

Active Cyber Defense (ACD)

Active cyber defense is “a set of operating concepts that involve taking the initiative and engaging the adversary in some way”¹⁵¹ including real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. Active cyber defense often refers to the conduction of operations in networks other than one’s own, which sets it apart from passive cyber defense.

Cyber Situational Awareness

Cyber situational awareness has four main components; to know what should be, to track what is, to infer when the two do not match, and to do something about the differences¹⁵². The goal is to understand the terrain within which cyber operations take place, and to make “risk management decisions based on threats and vulnerabilities to data, applications, systems, and networks that have the highest likelihood of impacting mission assurance”¹⁵³.

Operational Environment

Traditionally, an operational environment is a composite of the “conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander”¹⁵⁴. This usually refers to the weather, enemy, terrain triad (often referred to as W.E.T.). In the cyber domain, conditions, circumstances, and influence are quite different from those in the traditional military domains, but the concept still holds. The specifics of what the cyber operational environment looks like are detailed in a later section.

¹⁵¹ Irving Lachow. *Report*. Center for a New American Security, 2013. 3, Accessed July 31, 2020. www.jstor.org/stable/resrep06088.

¹⁵² Angela Horneman. *Situational Awareness for Cybersecurity: An Introduction*. 2019, September 09. Retrieved August 07, 2020, from https://insights.sei.cmu.edu/sei_blog/2019/09/situational-awareness-for-cybersecurity-an-introduction.html. N.p.

¹⁵³ Earl D. Matthews., Harold J. Arata, and Brian L. Hale. “*Cyber Situational Awareness*”. *The Cyber Defense Review* 1, no. 1 2016. 40.

¹⁵⁴ TC 7-102. *Operational Environment and Army Learning*. 2014.

The Attribution Problem

The attribution problem describes the difficulties that arise when attempting to identify cyber actors, particularly in the wake of a cyber-attack. In short, “the architecture of cyberspace makes it difficult to clearly determine those initially responsible for a cyber-attack as well as to identify motivating factors”¹⁵⁵. For example, even when it is possible to discover what servers were used for an attack, many states use proxies so it may be impossible to conclude that one specific state ordered the operation.

Active Cyber Defense (ACD)

Active cyber defense (hereafter ACD) focuses on the “integration and automation of services and mechanisms to execute response actions in cyber-relevant time”¹⁵⁶. Although many definitions of ACD include measures taken outside a state’s network, I will be focusing largely on intra-network defense with the ultimate goal of developing recommendations that can be adopted by individual states to better their defensive cybersecurity. Herring and Willett identify six functional aspects of ACD: sensing, sense making, decision making, acting, messaging and control, and mission management. Together, these six aspects provide a “capacity within cyber defense with the unique differentiator of providing situational awareness and response actions within cyber relevant time”¹⁵⁷. This enables a cyber actor (be it a government, or an organization) to understand the network landscape of the cyber domain in which they are operating in order to create continually updated defenses. Although no state or organization has yet to master all six of these aspects, the key operational gaps are largely found in the area of messaging and control¹⁵⁸.

¹⁵⁵ Myriam Dunn Cavelty. “*The Militarization of Cyberspace: Why Less May Be Better*”. International Conference on Cyber Conflict, 2012. 146.

¹⁵⁶ MJ Herring, et. al. “*Active Cyber Defense: A Vision for Real-Time Cyber Defense*”. 46.

¹⁵⁷ *Ibid.*, 50.

¹⁵⁸ *Ibid.*, 49.

Messaging and control are also crucial to the foundation of ACD; situational awareness, which relies on the ability of a network to communicate within itself and create a system of automated sense-making and response, thereby increasing the capacity for automated response actions. Cyber situational awareness is the result of “a dynamic process of perceiving and comprehending events in an environment”¹⁵⁹ which enables reasonable projections of how the environment may change, and “predictions concerning future circumstances and outcomes”¹⁶⁰. This ability for event and action projection within the cyber domain is unique to ACD and must be fostered in order to develop effective cyber defense.

Situational awareness is central to all military operations, but it is of particular relevance to ACD because it requires the ability to “understand mission dependencies and threat landscapes”¹⁶¹ that are unique to the cyber domain and constantly changing. The networks within which the cyber domain operates change constantly, and as a result, cyber defense cannot simply consist of static and dated defense measures such as keeping computers within a network updated (although software and hardware updates are also important). The approach to cyber situational awareness must reflect the ever-changing domain it is attempting to analyze. For all of the abovementioned reasons, addressing the gaps in messaging and control should be a priority if the goal is to establish effective and sustainable cybersecurity.

These gaps are primary a result of a lack of integration, specifically the “lack of a standard communication medium to interconnect all ACD-related tools at cyber relevant speed and scale, interface for tool connection to the common communications medium, and the lack of a standard message set understandable and actionable by all connected tools”¹⁶². A lack of standardization across a single network can cause inefficiency, and sometimes even miscommunication. The cyber-realm is constantly

¹⁵⁹ Martin R. Stytz. et. al. “*Toward Attaining Cyber Dominance*”. 61.

¹⁶⁰ Ibid.

¹⁶¹ Earl D. Matthews., et. al. “*Cyber Situational Awareness*”. 39–40.

¹⁶² MJ Herring. “*Active Cyber Defense: A Vision for Real-Time Cyber Defense*”. 49–50.

shifting, and this lack of efficiency is at the core of the work that needs to be done by individual states to establish real-time cyber situational awareness and effective ACD.

If this standardization problem can be remedied, all ACD-related tools will “have the ability to make each other aware of current activity...and to coordinate response actions”¹⁶³. The result will be a system of ACD that is increasingly automated, which will not only save limited resources, but also boost the effectiveness of a defense-oriented cybersecurity. By allowing for “automated synthesis of...monitoring information from across your enterprise infrastructure, operational and intelligence processes, and applications”¹⁶⁴, ACD will be able to maintain cyber-relevant speed in its establishment of situational awareness, thereby improving cybersecurity more broadly. I am by no means suggesting that ACD become completely automated as the associated risks are too great. A fully automated defense system would remove the ability of a human to act as an intermediary for decision making. Such a system is at risk of massively miscalculating a threat, which could result either in escalating a relatively benign threat into a full-scale cyber conflict, or, alternatively, undercalculating the risk of a threat. That being said, the increasingly self-sufficient nature of aspects of ACD will allow for human analysts to focus their attention on sense- and decision-making instead of data synthetization and basic communication.

Operational Environmental Preparation (OEP)

Identifying the operational environment in the cyber domain is a complicated task. In traditional military domains, the main characteristics of the operational environment are the weather, the enemy, and the terrain. In the cyber domain, however, the enemy is often obscured (due to the attribution problem). Moreover, considerations of “weather” and “terrain” are necessarily different in a domain that does not always operate in the physical realm. To understand how to better prepare the operational

¹⁶³ Ibid., 49.

¹⁶⁴ Earl D. Matthews. et. al. “*Cyber Situational Awareness*”. 40.

cyber environment, the concept of operational environmental preparation (hereafter OEP) can be adapted to the cyber domain by analyzing how the ideas of “weather” and “terrain” fit within that construct.

In the cyber domain, “weather” can be understood as patterns of user behavior, which affect the speed and efficiency of a network. Background traffic, for example, is considered “noise” from the standpoint of cyber operations, because it does not directly contribute to a mission and makes it more difficult to focus on a particular behavior¹⁶⁵. Users “generate traffic in arbitrary manner, but one that still follows a pattern”¹⁶⁶, and as such, behavior can be understood in patterns that can be equated to weather in an abstract sense.

The “terrain” on which users operate in the cyber domain can be seen as the established cyber infrastructure, which includes but is not limited to computing systems, data storage systems, software in use, network policy, and access control rules^{167, 168}. These elements are linked together by networks, which make up the cyber “terrain”. The ability of the enemy to traverse cyber terrain can be assessed in the way actors are able to navigate the network. The combination of “weather” or behavioral patterns, and “terrain” or the layout of the cyber network together form the cyber OEP, within which all cyber operations occur.

The traditional understanding of OEP again assumes the inevitability of offensive operations. Cyber OEP, however, also possesses the ability to also enhance cyber defense. The concepts of behavioral patterns and network organization are intricately linked and can be used to prepare the cyber OEP for defensive operations. Understanding cyber “weather” and “terrain” allows for the creation of a matrix “linking an enemy’s likely course of

¹⁶⁵ Antoine Lemay, Scott Knight and Jose Manuel Fernandez. “Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace”. *Journal of Information Warfare* 13 no 3. 2014. 49.

¹⁶⁶ Antoine Lemay, et. al. “Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace”. 49.

¹⁶⁷ William J. Lynn. “Defending a New Domain: The Pentagon’s Cyberstrategy”. N.p.

¹⁶⁸ Martin R. Stytz. et. al. “Toward Attaining Cyber Dominance”. N.p.

action, [and] indicators of those courses of action”¹⁶⁹. By creating indicators that fingerprint an adversary’s course of action, it is possible to determine the goal an enemy is pursuing, and even allow for network modification in order to force an enemy into a certain course of action—an extremely valuable ability in the quest to establish effective cyber defense¹⁷⁰.

In order to be able to create course of action indicators, it is essential to understand how an actor’s behavior (weather) is affected by a given network (terrain). Real-time cybersecurity exercises “provide an ideal platform for studying adversary-defender interactions”¹⁷¹. These exercises can be used to better understand “human behavior, decision making, and adaptation”¹⁷², and can help identify patterns that can be adapted into intrusion chain stages. Key moments of “decision-making, facing hurdles, and corresponding adaptations”¹⁷³ allow researchers to capture dynamic aspects of human behavior within the cyber domain, which becomes useful in creating a more robust and resilient operational environment. Although these exercises are not representative of reality given their isolated and controlled nature, they still allow for insights that can be hugely beneficial to establishing cyber OEP.

Acquiring a deep understanding of the cyber operating environment and the relationship between users and the environment should be the primary aim of cyber OEP. The better we are able to understand the cyber operational environment, the easier it will be to develop a course of action indicators, and thereby create stronger cyber defense capabilities. The result will be a transition away from an offensive cyber orientation and towards a defensive orientation, which will be more resource-efficient and sustainable.

¹⁶⁹ Antoine Lemay, et. al. “*Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace*”. 55.

¹⁷⁰ Ibid.

¹⁷¹ Geoffrey B. Dobson, Aunshul Rege, and Kathleen Carley. “*Informing Active Cyber Defense with Realistic Adversarial Behaviour*”. *Journal of Information Warfare* 17, no. 2. 2018. 18.

¹⁷² Ibid.

¹⁷³ Ibid.

Recommendations

Standardization

There is a pressing need for a common communication medium, standard interface tool, and standard message set in order to ensure that data flows are integrated “into a continuous monitoring platform”¹⁷⁴, thereby boosting network efficiency and heightening situational awareness. Achieving this standardization goal will require engaging governmental agencies, commercial vendors, industry leaders in security and technology research, as well as the appropriate usage of governing bodies, civil agencies, and the intelligence community.

If this standardization is successful, it will allow for data collection to be used more efficiently across cybersecurity priorities. This will enable ACD to be more efficient by allowing for inter-system communication and response, thereby furthering situational awareness. Additionally, this data can help improve cyber operational preparedness by compiling existing patterns of user behavior (weather) from within a network. Standardization can also aid in understanding the layout of cyber infrastructure (terrain) by increasing the efficiency of systems in their ability to understand the networks within which they operate. This will further the ability to predict potential changes in behavioral patterns and the network, thereby improving cyber operational preparedness.

More Cybersecurity Exercises

Executing more cybersecurity exercises and collecting information about how actors behave in the cyber domain is crucial to the pursuit of cyber OEP. These exercises allow for the creation of course of action indicators which can provide clues about an enemy’s ultimate aims and enable preemptive defense operations. Cybersecurity exercises also provide an excellent opportunity to assess vulnerabilities in the cyber “terrain” and address them before they can be exploited.

¹⁷⁴ Earl D. Matthews. et. al. “*Cyber Situational Awareness*”. 40.

Cybersecurity exercises also provide an opportunity to increase situational awareness and integrate ACD with other aspects of cybersecurity. ACD follows the principle of “collect once and reuse many”¹⁷⁵, which means that any data collected through cybersecurity exercises will be used and reused until it is outdated, making it a valuable defense resource. Within ACD there is a great “motivation to reuse...data in as many decision-making paths as is applicable”¹⁷⁶, which promotes smart and efficient workflow. The use of these exercises can increase network efficiency and expose areas of active defense that require further development.

Cyber Security Community

To establish a strong and sustainable defensive cybersecurity orientation, it is necessary to also establish a collective cybersecurity community in which data and best practices are shared. The cyber domain cannot be relegated to geographical boundaries, and as a result, it cannot be fully “owned” by any one state. With the introduction of a network of states, ACD has the ability to take action outside of a single state network, which allows for a host of additional active defense measures. The larger the network of resources in play, the better a given ACD will be, enabling the group to strengthen and prepare the cyber OEP in their own best interest. A cybersecurity community would provide an opportunity to address some of the most basic problems of cybersecurity, such as the creation of clear and cohesive definitions, system of laws surrounding cyber warfare, and addressing the attribution problem. In answering these basic questions, the ability of such a community to create a strong, sustainable defensive cyber operation will be optimized.

Conclusion

Today, there are still massive gaps in the ability of cybersecurity to protect state and organizational networks and adapt to threats in cyber relevant

¹⁷⁵ MJ Herring, et. al. “*Active Cyber Defense: A Vision for Real-Time Cyber Defense*”. 48.

¹⁷⁶ Ibid., 49.

time. To create effective and sustainable cybersecurity, a defensive orientation must be adopted. This paper analyzed the most vulnerable areas of ACD and cyber OEP and identified three areas that provide an opportunity for resource overlap to make the pursuit of effective cybersecurity more efficient and less costly. In adopting these recommendations, the quest for effective and sustainable cyber defensive capabilities can be furthered by allowing for the best chance of cyber threat prevention through ACD while analyzing the behavioral patterns and network activity of potential cyber enemies through cyber OEP. The result will be an increasingly resilient, efficient, and sustainable cybersecurity.

Shaping Future Internet Policy: Balancing Freedom and Security Through Globalization

Sarah GOSSETT

Abstract: Information Communication Technology (ICT) advancements have a significant effect on the balance of international security and freedom. This relationship has exposed a pattern of waves in the levels of social, economic, and political globalization over the last century. Nations have failed to adapt to rapid societal changes and to understand the pattern and its relationship to international security, freedom, and human rights, only delaying and increasing the risk of global instability. The internet is the most recent ICT advancement, but its unprecedented capabilities have made it difficult to anticipate social, economic, and political effects when left improperly regulated. Finding a solution at the international level requires finding a middle ground with potential to benefit all countries. Every country's unique condition makes it impossible to find a strict one-size-fits-all approach to internet regulation. Factors such as development, location, history, culture (traditions and morals), and governance must be taken into account and used to establish boundaries for the minimum and maximum levels of internet regulation. The actions needed to combat internet threats to security (misinformation, calls for violence, hacking, and cyber attacks) and individual freedom (suppressed, private data collection, threats to journalists, and excessive censorship) will require sacrifices to both to find a suitable balance. Extreme internet freedom or censorship will continue to deteriorate global stability by pushing public opinion toward nationalism and isolationism. Failure to maintain and improve globalization through balanced international internet policies provoke single-stakeholder control to threats such as internet sovereignty, access monopolization, and the privatization of human rights. This article seeks to further explain these relationships and offer recommendations for a long-term, balanced approach with defined minimum and maximum levels of internet regulation through the comparison of biases and internet

policies between the United States, the European Union, and China, as well as policies established by the United Nations and private sector.

Keywords: Internet, Internet policy, WWW, World Wide Web

*“Those who would give up essential Liberty,
to purchase a little temporary Safety,
deserve neither Liberty nor Safety.”*

Benjamin Franklin, 1775

Introduction

The words of Benjamin Franklin helped shape the foundation of constitutional rights in the United States and rang true for nearly a century. However, the rapid advancements in information communication technology (ICT) since the late 20th century are far beyond what even he could have imagined. For years, the average speed and reach of information have outpaced the ability of individual countries and the international community to comprehend and combat new technological developments’ negative effects. There is no end for the evolution of technology, and no turning away from the reality of the internet’s power and the grasp it has on world order. Public policy, security, and technology experts must track and stay ahead of these trends and work together to find solutions to prevent growth from being our own demise. The global network the internet has built is far too intricate and integrated for one nation to abandon without detrimental consequences for all¹⁷⁷.

Sir Tim Berners-Lee, the creator of the internet, has expressed his concern for the future of the internet and the need for all nations to work together to develop modern laws for the digital age that balance freedom and security for all¹⁷⁸. Misinformation, election interference, calls for violence,

¹⁷⁷ George Soros. “The Crisis of Global Capitalism: Open Society Endangered” New York: Public Affairs. 1998.

¹⁷⁸ Tim Berners-Lee, 30 years on, what’s next #ForTheWeb? 2019. Accessed August 23rd, 2020. <https://webfoundation.org/2019/03/web-birthday-30/>.

cyber-crimes, and illegal markets are among the most common activities. The long-term lack of consensus on how to properly monitor and manage online activity to ensure international security without damaging social structures and economic growth is leading to a tipping point for globalization. Anticipating the issues that come with ICT and the waves of globalization with these recommendations in mind will ensure long-term security and protection of freedoms. No matter the approach, there needs to be action in the international community on internet regulations for the sake of international stability.

Waves of Globalization

Today, the internet expands the base of global knowledge and offers numerous benefits and opportunities for growth. Economically, the internet provides the means for companies thousands of miles apart to communicate, increases productivity and competitiveness, and opens the job market for remote work opportunities. Socially, the internet opens up global communication at the individual level, allowing anyone with internet access to interact with someone across the globe and increase their exposure to new ideas, cultures, and information. Politically, most news organizations can instantly broadcast to anywhere in the world, keeping those with internet access up to date on current events¹⁷⁹.

While there are numerous positive aspects of the internet, there seems to be a never ending list of issues that, if left unaddressed, could leave a policy gap that could become impossible to fill. Before the internet, the most significant downsides of new ICT developments throughout history have stemmed from their most positive aspect – creating a more connected, globalized world. Unfortunately, faster and easier communication always comes packaged with a higher risk of tension and conflict due to ethical and cultural differences¹⁸⁰. These changes tend to stoke fears of

¹⁷⁹ Richard Baldwin. "The Great Convergence: Information Technology and the New Globalization". (Belknap Press of Harvard University Press. Cambridge, MA) 2016.

¹⁸⁰ Michelle Maiese. "Moral or Value Conflicts". *Beyond Intractability*. Conflict Information Consortium, University of Colorado, Boulder. 2003.

change and unfamiliarity, giving rise to the preference of protectionism, isolationism, and nationalism over globalization when expansion and oversaturation become too much for a population to handle¹⁸¹. Experts have observed this cycle of global connection and disconnection – known as the Waves of Globalization – three times within the last century¹⁸².

The first wave of growth began with introducing the telegraph in the late 19th century kick starting the Industrial Revolution and making long distance communication faster than ever before. However, the capability of speedy international communication might have been a factor in increasing global tensions that led to conflict on a global scale – World War I. In the aftermath of the war, globalization was set aside as nations withdrew themselves from the international community in favor of isolationism and protectionism¹⁸³. Not long after, satellites and telephones launched the second wave and eclipsed the speed of the previous globalization growth – more so for developed countries than developing countries – and revealed the need for regulated international economic integration following the financial toll of World War II. The Bretton Woods Agreement secured the United States' role as the global hegemon. This wave took its downturn after the Vietnam War ended the Bretton Woods Agreement and prompted the growth of isolationism again¹⁸⁴. The third wave began in the late 1980s and early 1990s as the internet became increasingly available to the general population, and the Cold War came to an end. Based on this pattern, another downturn in globalization is likely to occur in this decade for nations with earlier access to the internet, while those previously left behind are catching up¹⁸⁵. We have already witnessed this shift

¹⁸¹ Diane Coyle, Patrick Meier, "New Technologies in Emergencies and Conflicts: The Role of Information and Social Networks". United Nations Foundation; Vodafone Foundation. 2009.

¹⁸² World Bank, 2001.

¹⁸³ Adam Tooze, "The Deluge: The Great War and the Remaking of Global Order 1916–1931". (Penguin, London.) 2015.

¹⁸⁴ James A. Johnson "The New Generation of Isolationists". Foreign Affairs 49, No. 1, pg. 136. 1970. <https://doi.org/10.2307/20037824>.

¹⁸⁵ Sey, A., Coward, C., Bar, F., Sciadas, G., Rothschild, C., & Koepke, L. "Connecting people for development: Why public access ICTs matter". Seattle: Technology & Social Change Group, University of Washington Information School. 2013.

for the last couple of years as some of the most connected global powers have shifted away from involvement in the international community as disputes over cyberspace and freedom of information become the new norm.

In this fourth wave of globalization, less developed countries, formerly left behind in this long race for technological advancements and global influence, are now quickly catching up at varying rates. Most of these countries are experiencing high growth rates of economic impact, intercultural competence, and technology adoption. This makes this wave challenging to predict and regulate as it fractures and deviates based on various factors, including governance and level of development. There is a push for nations to favor a globalized internet over “internet Balkanization” because “internet fragmentation will bring about a paradoxical de-globalization as communications within national borders among governmental bodies and large national companies become increasingly localized.”¹⁸⁶ To stay ahead of this curve, international policymakers must carefully consider and thoroughly grasp the roots of decisions made by the leaders of those countries, to determine the range of positive and negative effects at all levels of internet control.

Control+Alt+Delete

Governments’ have justified the development of policies and laws used to place restrictions on cross-border flows of data, monitor citizens’ online activity, and control what can be accessed, especially regarding social media for the sake of national and personal security¹⁸⁷. Many of these types of policies are necessary, but to what extent? Every nation faces different circumstances and has different needs. Establishing effective and fair policies at the international level requires taking these differences into account, understanding the motives behind current internet policies, and

¹⁸⁶ Milton Mueller, *“Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace”*. John Wiley & Sons. 2017. <https://doi.org/9781509501250>.

¹⁸⁷ Adrian Shahbaz, and Allie Funk. “The Crisis of Social Media”, 2019. <https://freedomhouse.org/report/freedom-net/2019/crisis-social-media>.

finding a balance between security and freedom that does not impede the quality of life, development, and growth.

The Great Firewall

Regarding external influences, China's Great Firewall is often seen by western nations as a means of authoritarian control to prevent the Chinese population from being exposed to external cultures, ideologies, and information. But, censorship of outside media has actually improved the average quality of life, most notably from the stability it provides¹⁸⁸. Today's open internet, especially social media, has caused significant fragmentation in oversaturated nations due to millions of people vying for attention and their opinions to be heard. Those desperate for attention may resort to radicalization and misinformation. Compared to the West, China has only recently become a technologically advanced nation, and its infrastructure did not offer internet access to half of the population until 2016¹⁸⁹. In recent studies, Chinese students were given unrestricted internet access for 18 months. The results showed that "the combination of low demand for uncensored information and the moderate social transmission means China's censorship apparatus may remain robust to a large number of citizens receiving access to an uncensored Internet."¹⁹⁰ The participants displayed "self-censorship" and showed no interest in accessing uncensored information on their own. When uncensored and inappropriate information – think annoying pop-up advertisements – persistently show up on users' screens, it is hard to miss. The restrictions on information flows, and the consequences journalists and individuals face if a line is crossed, undoubtedly violate human rights. If China desires to be of higher value to and more respected by the international community it needs to reduce restrictions to fit within boundaries suggested in this article.

¹⁸⁸ Guo, S., Feng, G. "Understanding Support for Internet Censorship in China: An Elaboration of the Theory of Reasoned Action". *Journal of Chinese Political Science* 17, 33–52. 2012. <https://doi.org/10.1007/s11366-011-9177-8>.

¹⁸⁹ Max Roser, Hannah Ritchie and Esteban Ortiz-Ospina. "Internet". *OurWorldInData.org*. 2015. '<https://ourworldindata.org/internet>'.

¹⁹⁰ Yuyu Chen, and David Y. Yang. "The Impact of Media Censorship: 1984 or Brave New World?" *American Economic Review*, 109. 2019. doi: 10.1257/aer.20171765.

Building Connections

Chen and Yang's first two observations are undeniable, but free, open access to the internet is not the only way to expose individuals to new information¹⁹¹. However, their latter two points are debatable. Those who argue that the Chinese government seeks to shelter its citizens from the world and control their every thought and opinion neglect to take other means of increasing globalization into account. As their economy grows and citizens have more disposable income, Chinese citizens have been traveling internationally – now ranked the second largest group of tourists, following closely behind the United States¹⁹². The government highly encourages international travel and education so that its citizens can experience the world. Non-Chinese students are eagerly welcomed and offered scholarships to Chinese universities. In 2016, China ranked third globally for the number of international students, closely behind the United States and the United Kingdom. This number will continue to grow as 40 percent of all new international students received sponsorship from the Chinese government, a five-fold increase from 2006¹⁹³. The hope is that face-to-face intercultural interaction will improve China's reputation by giving the world every opportunity to experience, understand, and appreciate their culture and perspective. This diplomacy through education approach worked for some time, but the rise of nationalism is destroying progress¹⁹⁴.

The majority of Chinese citizens understand how censored they are and aware of human rights violations. Yet, while engrained self-censorship

¹⁹¹ "(i) free access alone does not induce subjects to acquire politically sensitive information; (ii) temporary encouragement leads to a persistent increase in acquisition, indicating that demand is not permanently low; (iii) acquisition brings broad, substantial, and persistent changes to knowledge, beliefs, attitudes, and intended behaviors; and (iv) social transmission of information is statistically significant but small in magnitude". Chen, Yuyu, and David Y. Yang. "The Impact of Media Censorship: 1984 or Brave New World?" 2019.

¹⁹² Diana Munoz Robino, Global Destination Cities Index. 2019.

¹⁹³ "Is China Both a Source and Hub for International Students?" ChinaPower Project, March 12, 2020. <https://chinapower.csis.org/china-international-students/>.

¹⁹⁴ Salvatore Babones. "It's Time for Western Universities to Cut Their Ties to China". Foreign Policy. August 19, 2020. <https://foreignpolicy.com/2020/08/19/universities-confucius-institutes-china/>.

limits their desire for some information, many agree that these extreme policies are far beyond unacceptable. Being abroad exposes you to knowledge, beliefs, and attitudes, planting the seed for the spread of information and attitudes in the long run. However, even as Chinese citizens are increasingly exposed to Western culture, their government controlled news media is ranked the most trusted in the world¹⁹⁵.

The Road Ahead

The regimes of many vulnerable and developing countries are adopting stricter models of censorship because they realize how unrestricted access to internet media can negatively affect their stability and damage development progress¹⁹⁶. Through censorship, China has created a stable situation that has lifted millions out of poverty and allowed the government to concentrate on continuing development¹⁹⁷. China's levels of globalization are increasing socially, economically, and politically, but Evan Osnos, reporter for *The New Yorker*, observed that "to the degree that China's connection to the outside world matters, the digital links are deteriorating."¹⁹⁸. Although this level of censorship is viewed as over aggressive, it is necessary, to an extent, to keep the cohesion of its population for the time being. In the coming years, China will likely meet in the middle with other nations as democratic nations continue to implement policies and regulations as they recognize the increasing dangers of misinformation and abuse of power that comes with the unrestricted flow of information through the internet. There are still many issues with China's internet policies, especially concerning human rights and freedom of the press. Yet, the West's policies do not represent the ideal foundation for international ICT policy. These nations must be aware of their own growing faults before casting

¹⁹⁵ "2020 Edelman Trust Barometer". Edelman. 2020. <https://www.edelman.com/trustbarometer>.

¹⁹⁶ Kazeem B. Ajide & Ibrahim D. Raheem. "Does Democracy Really Fuel Terrorism in Africa?" *International Economic Journal*, 34:2, 297–316. 2020. DOI: 10.1080/10168737.2020.1741014.

¹⁹⁷ "World Report 2020: Rights Trends in China's Global Threat to Human Rights". April 10, 2020. <https://www.hrw.org/world-report/2020/country-chapters/global>.

¹⁹⁸ Evan Osnos, "Born Red". *New Yorker*. 2015. <https://www.newyorker.com/magazine/2015/04/06/born-red>.

stones. Press freedom has been deteriorating globally over the last decade, and it is not only the nondemocratic regimes to blame¹⁹⁹.

The World-Wide West

Regardless of the regime, most nations have policies already in place that censor certain websites, block language deemed inappropriate, track illegal activity, and restrict or remove misinformation on social media²⁰⁰. Within democratic nations, the issues with most of these policies are details and stipulations that are either too vague to effectively hinder those searching for a loophole or lack means of enforcement. In this realm, policy and law are necessary to maintain security and growth on the national and international levels. However, these policies' reach is only acceptable if applied in a realistic manner that balances freedom and security without reducing levels of globalization. Members of the European Union are among those that have implemented the most effective practices with favorable results. Europe has been rising to the forefront of internet policy over the last few years.

A Dangerous Precedent

In 2016, Eva Glawischnig-Piesczek, former federal chairperson of the Austrian parliamentary party, had a photo of herself attached to a viral Facebook article calling her corrupt, fascist, and a traitor. Glawischnig-Piesczek demanded Facebook delete the posts and reveal the identity of the publishing user. After Facebook refused, she took her case to the Austrian Supreme Court, arguing that the comments were defamatory and violated the copyright she held of her image. Under existing Austrian law, Glawischnig-Piesczek's case was sufficient enough for Facebook Ireland Ltd. to be ordered to remove the post, as well as similar posts, from the

¹⁹⁹ Reporters Without Borders ranked China 176 out of 180 countries in its 2016 worldwide index of press freedom. <https://www.cfr.org/backgrounders/media-censorship-china>.

²⁰⁰ Róisín Áine Costello. "Law, Policy and the Internet". *International Journal of Law and Information Technology*, 204–207. 2019.

platform. However, Facebook Ireland Ltd. is governed by the United States and Ireland. Both parties chose to appeal the verdict and took the case to the Court of Justice of the European Union (CJEU).

The key deciding factor was the interpretation of Article 15 of the Directive 2000/31/EC to determine if a host provider can be forced to extend the removal of a post with identical verbiage or identical content, and the order can be extended to apply worldwide. The Court strengthened relating definitions and ruled that the Directive does not prevent a host provider from being ordered to remove content deemed unacceptable or unlawful and any identical or similar content as long as the provider does not make these assessments independently. As to the question of if these laws can be applied internationally, the Court ruled that Article 18 of the Directive leaves the power to determine the geographic scope of the restriction up to the EU Member state, as long as it remains within the framework of relevant international law²⁰¹. A decision like this in the United States would be viewed as undermining existing law and violating individual freedoms, not to mention that it is unconstitutional.

Comparing Approaches

Countries most invested in the information economy and intellectual property with large knowledge producing sectors are those actively restricting their citizens' access to information²⁰². In addition, countries with similar governmental structures pressure one another to match the others' level of internet control. The United States is among these countries, but it takes an under-the-radar approach to information security, data privacy, press freedom, and misinformation control. There is a lack of focus on protecting both nongovernmental organizations and individuals from cyber attacks

²⁰¹ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN>.

²⁰² Stephen A. Meserve, and Daniel Pemstein. "Google Politics: The Political Determinants of Internet Censorship in Democracies". *Political Science Research and Methods* 6, no. 2 (2017): 245–63. [tps://doi.org/10.1017/psrm.2017.1](https://doi.org/10.1017/psrm.2017.1).

and other internet threats. Russia's influence in the 2016 election is being taught as a case study at European universities as the most significant cyber scandal in history. Yet, little has been done to combat these disinformation campaigns and the spread of misinformation since the United States is again falling victim to interference during the 2020 election. The desire for complete freedom of opinion and expression causes many to bury the truth from themselves and spread information that confirms their biases, no matter how farfetched and unverified it may be – an effect explained by the Selective Exposure Theory²⁰³.

The United States has criticized China's intense surveillance of its citizens for years, but this is one of the most hypocritical American points of view. To the degree that China admits to surveilling its citizens, it is somewhat more open in comparison to the United States. Actions on both sides cross ethical lines in terms of privacy, especially China. However, the majority of user data requests sent to Google, Facebook, Apple, and Twitter come from the United States government. In 2012, Twitter received twice as many requests for its users' data from the United States government than the next six countries combined²⁰⁴. In addition, the Trump Administration has created a hostile environment for the press and news media organizations. Between 2018 and 2019, the United States fell three places into the "problematic" classification on the World Press Freedom Index²⁰⁵. In 2018, the United States tied with India as the fifth most dangerous country for journalists in a report by Reporters Without Borders²⁰⁶.

One of the key indicators of a corrupt democracy is a government that works to impede press and intellectual freedom²⁰⁷. Similar to authoritarian

²⁰³ Natalie Jomini Stroud. "Selective Exposure Theories". *Oxford Handbooks Online*, 2014. https://doi.org/10.1093/oxfordhb/9780199793471.013.009_update_001.

²⁰⁴ Twitter Transparency Report, Accessed August 25, 2020. <https://transparency.twitter.com/en/reports/information-requests.html#2019-jul-dec>.

²⁰⁵ "2019 World Press Freedom Index – A Cycle of Fear", April 21, 2020. <https://rsf.org/en/2019-world-press-freedom-index-cycle-fear>.

²⁰⁶ Reporters Without Borders. "WORLDWIDE ROUND-UP of journalists killed, detained, held hostage, or missing in 2018". 2019.

²⁰⁷ Jonathan A. Solis and Philip D. Waggoner. 2020. "Measuring Media Freedom: An Item Response Theory Analysis of Existing Indicators". *British Journal of Political Science*. Cambridge University Press, 1–20. doi:10.1017/S0007123420000101.

regimes, these governments aim to control public knowledge by restricting access to materials, promoting information that confirms their message, and covering up their mistakes. Research shows that “governments engage in more digital censorship when internal dissent is present and when their economies produce substantial intellectual property.”²⁰⁸ As technology drives globalization and the United States and China try to outpace one another in research and development, we can observe how these two regimes contrast in balancing security and freedom. The desire to control information to protect intellectual property and cybersecurity is not the only motivation for democratic nations to establish reactive policies due to other national threats.

Proactive vs. Reactive Policy

In 2018, after the dangerous example made of the United States two years prior, the European Commission implemented measures to ensure that European elections remain free and fair. The Commission’s formal recommendation outlined the need for election cooperation networks, digital transparency, protection against cybersecurity incidents, and combating disinformation campaigns²⁰⁹. While these measures were motivated by the result of another democratic nation falling victim to foreign intervention in elections, other European internet and security policies have been motivated by their own misfortunes; one implemented proactively while the others are reactive. No matter the regime, governments tend to increase internet restrictions as a response to internal threats.

In Stephen Meserve and Daniel Pemstein’s award-winning article “*Google Politics: The Political Determinants of Internet Censorship in Democracies*”, the authors explain that “internet freedom in liberal democracies is sensitive to internal threats, and that democratic governments, like their

²⁰⁸ Stephen A. Meserve, and Daniel Pemstein. “Google Politics: The Political Determinants of Internet Censorship in Democracies”. *Political Science Research and Methods* 6, no. 2 (2017): 245–63. <https://doi.org/10.1017/psrm.2017.1>.

²⁰⁹ EUROPEAN COMMISSION RECOMMENDATION of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf.

autocratic counterparts, restrict digital freedom when faced with terrorism and insurgency.”²¹⁰ As an example, France increased its number of strict ICT regulations on digital content that led to mass censorship and decreased internet freedom and began to lean toward isolationism, protectionism, nationalism. Many other European nations have begun to follow suit. As events and restrictions such as this continue to escalate, the developed world will see its decline in the waves of globalization, as predicted, with developing nations following soon after. Policymakers must be proactive in their decisions regarding control of the internet to advance international freedom, security, and growth. If not, they will continue to set standards that can be viewed as questionable or unclear to the point that, if applied at the international level, may lead corrupt leaders with bad intentions to search for loopholes to take advantage of the situation and to advance and protect their interests. Internal threats are not the only causes of rushed, inadequate internet policy. As new situations appear, policymakers and legal establishments are pressured to decide based on grievances, legal precedents, and little information on the internet’s framework and capability.

Measuring Trust

The growing distrust in tech companies, news organizations, and even experts is coinciding with a lack of media literacy that is exacerbating the growing political divide, threatening the nation’s stability, and disconnecting Americans from the world. Western nations like to believe that their respective news organizations are more trustworthy and honest than others, especially more than China’s news media. However, according to the 2020 Edelman Trust Barometer report²¹¹, Chinese media was ranked the most trustworthy in the world, and the majority of its citizens want to keep it that way²¹². The report shows developed nations declining in nearly

²¹⁰ Stephen A. Meserve, and Daniel Pemstein. “Google Politics: The Political Determinants of Internet Censorship in Democracies”. *Political Science Research and Methods* 6, no. 2, 245–63. 2017. <https://doi.org/10.1017/psrm.2017.1>.

²¹¹ “2020 Edelman Trust Barometer”. Edelman, 2020. <https://www.edelman.com/trustbarometer>.

²¹² Wang, D., and G. Mark. “Internet Censorship in China: Examining User Awareness and Attitudes”. 2015.

every category, leaning towards some form of protectionism and isolationism. Of the nations surveyed, 66 percent worry it will soon be impossible to know what is real, with 61 percent believing the pace of technology change is too rapid and that governments cannot adapt to this ever evolving sector enough to regulate it effectively²¹³. Compared to Americans and Europeans, Chinese citizens have become more accustomed to trusting their media, which makes them easy targets for external misinformation or propaganda campaigns. Even the United States fell victim to interference in the democratic electoral process during the 2016 Presidential Election. Perhaps in the coming years, China will be ready for lower levels of censorship, but there is a high risk of backsliding in its development progress without some level of regulation in its censorship policies.

Stakeholders

Technology can enhance or destroy democracy and development. It all depends on who is in control and how it is used. There are only a handful of companies that currently control the vast majority of technology and information flow. Internet governance experts are studying how a public-private multi-stakeholder approach can play a role in maintaining the balance of freedom and security within a globalized internet²¹⁴.

Social Media

As the United States government hesitates to take the lead on protecting social media users and combating misinformation, host platforms are taking it upon themselves to experiment with measures to regulate online activity within the boundaries of the First Amendment. The changes in the hierarchy of internet control since Denardis and Hackl conducted their research shines a light on whether internet policy is best approached as

²¹³ "2020 Edelman Trust Barometer". Edelman, 2020. <https://www.edelman.com/trustbarometer>.

²¹⁴ Jonathan A. Obar, and Steven S. Wildman. "Social Media Definition and the Governance Challenge – An Introduction to the Special Issue". *SSRN Electronic Journal* 39, no. 9 (October 2015): 745–810. <https://doi.org/10.2139/ssrn.2663153>.

“governance by social media rather than governance of social media.”²¹⁵. As of July 2020, over 50 percent of the world uses social media (3.96 billion users) and nearly 60 percent have internet access (4.57 billion users)²¹⁶. Social media platforms are at the center of internet activity and have more policies in place to improve transparency, combat misinformation, and target calls for violence²¹⁷. There is a concern in the field of internet governance that social media platforms are slowly encroaching upon the privatizing of human rights²¹⁸. However, many do not see this as a bad thing – within reason.

A poll released by Gallup and the Knight Foundation on public opinion of internet control and misinformation in 2020 shows that many Americans are facing internal conflicts in regards to many of their stances on media censorship, valuing freedom of speech yet more critical of companies that do too little to monitor harmful content than those who do too much²¹⁹. Recent surveys and studies show that most Americans favor more being done to eliminate misinformation and disinformation attacks that skew the accuracy of public knowledge and opinion²²⁰. Overall, U.S. public opinion favors social media host companies managing internet regulation over the government as these companies take action.

In 2016, Microsoft, Google, Apple, Facebook, and other companies sued the U.S. government for the legal authority to inform the public on what

²¹⁵ Denardis, L., and A.M. Hackl. “Internet Governance by Social Media Platforms”. *Telecommunications Policy* 39, no. 9 (October 2015): 761–70. <https://doi.org/10.1016/j.telpol.2015.04.003>.

²¹⁶ <https://datareportal.com/reports/digital-2020-july-global-statshot>.

²¹⁷ Dawn Carla Nunziato, *Misinformation Mayhem: Social Media Platforms’ Efforts to Combat Medical and Political Misinformation* (2020). 19 First Amendment L. Rev. ____ (2020), GWU Legal Studies Research Paper No. 2020–48, GWU Law School Public Law Research Paper No. 2020–48, Available at SSRN: <https://ssrn.com/abstract=3672257>.

²¹⁸ Emily Taylor. 2016. *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality*. GCG Paper Series No. 23 referring to Morozov 2014. https://www.cigionline.org/sites/default/files/gcig_no24_web_2.pdf.

²¹⁹ <https://knightfoundation.org/reports/american-views-2020-trust-media-and-democracy/>.

²²⁰ Dawn Carla Nunziato, *Misinformation Mayhem: Social Media Platforms’ Efforts to Combat Medical and Political Misinformation* (2020). 19 First Amendment L. Rev. ____ (2020), GWU Legal Studies Research Paper No. 2020–48, GWU Law School Public Law Research Paper No. 2020–48, Available at SSRN: <https://ssrn.com/abstract=3672257>.

information the U.S. government collects on them²²¹. These companies were successful in arguing the Fourth Amendment and offering transparency reports on user data. Individually, platforms have their own approaches to combating misinformation. This year, Twitter was in the spotlight for its policies after it removed and labeled tweets from President Donald Trump's as misleading and violent. After becoming the center of misinformation during the 2016 election, Facebook developed a network of independent fact-checkers around the world monitor posts. Google's search algorithms are currently removing misinformation on the 2020 election and frontloading information on COVID-19 from trusted health authorities. These are milestones for improving internet regulation, but the inconsistency between platforms in their dedication to the cause and definitions of what is considered "misinformation" could damage freedom in the long run.

Network Providers

In 2018, the Federal Communications Commission's Restoring Internet Freedom Order provided a "framework for protecting an open Internet while paving the way for better, faster, and cheaper Internet access for consumers."²²² This was a step in the right direction for regulatory reform, but there are many arguments against this decision to eliminate net neutrality²²³. The most notable concern regarding a lack of net neutrality is service providers' ability to control users' access to content. However, transparency requirements seem to have replaced some former data regulations. Policies such as this benefit the future of internet policy in the long term. Similar to the issue of inconsistency in regulation between social media platforms, network providers themselves must establish the same rules across the board. Inconsistency between regional network providers

²²¹ Microsoft Corp v United States Department of Justice et al in the United States District Court, Western District of Washington, No. 2:16-cv-00537.

²²² <https://www.fcc.gov/restoring-internet-freedom>.

²²³ Net neutrality is the principle that an internet service provider (ISP) has to provide access to all sites, content and applications at the same speed, under the same conditions without blocking or preferencing any content.

is far more dangerous than growing inconsistency between nations and the “Balkanization” of the internet^{224, 225}.

Private Sector

Achieving consistency between organizations is difficult, especially in bureaucratic matters. The answer to a globalized internet access network might not lie in interorganizational and international cooperation at the policymaking level, but in having single internet source. Space X’s Starlink satellites are designed to be “unblockable” and able to “provide high-speed, low-latency broadband connectivity across the globe, including to locations where the internet has traditionally been too expensive, unreliable, or entirely unavailable.”²²⁶ The company’s goal is to put approximately 2,000 smaller satellites in orbit by the end of 2021. If successful, the remaining 40% of the global population without the internet will have access. This will change the course of human history and the central cultural framework of the internet. Space X will have to be prepared to defend its decisions against critics and policymakers, its equipment from damage, and its information from corruption.

International Oversight

The United Nations should be responsible for establishing international internet regulations. Many of the necessary actions would go against articles in the Universal Declaration of Human Rights, but there have been dozens of unfulfilled requests for amendments. It was drafted with the intent to prevent another global conflict after World War II, but these rules have not been equally or regularly enforced since their inception. Even Western

²²⁴ Jonah Hill, Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers (May 20, 2012). Berkman Center Research Paper, Harvard Belfer Center for Science and International Affairs Working Paper, Available at SSRN: <https://ssrn.com/abstract=2439486>.

²²⁵ Victor W. Pickard, and David Elliot Berman, *After Net Neutrality: a New Deal for the Digital Age*, New Haven: Yale University Press, 2019.

²²⁶ “Astronomy discussion with national academy of sciences”, SpaceX, Accessed August 25, 2020. <https://www.spacex.com/updates/starlink-update-04-28-2020/>.

nations, especially the United States, have been exempted for actions that clearly defy multiple articles in this declaration.

In regards to internet freedom, Articles 19 forbids limitations on an open and free internet, stating: “Everyone has the right to freedom of opinion and expression; including the freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers.”²²⁷ Articles 12 and 29 state that individuals have the right to protect their reputation and the responsibility to respect others’ rights and freedoms. To ensure security and stability for all nations, amendments must be added to update and clarify these limitations to protect the world from modern threats. Freedom and security can and must be balanced and of lasting quality to international internet policy.

The most recent updates to the United Nations’ Partnership on Measuring Information and Communication Technology for Development 2030 Agenda for Sustainable Development recognize that “the spread of information and communications technology and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies”²²⁸. This shows that the leading international organization sees how globalization depends heavily on security, growth, and freedom concerning the internet. In addition to this commitment, global trust ratings of the United Nations have been increasing.²²⁹ The task of establishing and enforcing standards of internet policy for all nations will likely damage this rating as many sides will make sacrifices. To minimize the loss of trust and credibility, the United Nations must seek out experts in each of their ICT indicators.

²²⁷ Declaration of Human Rights, UN, Accessed August 25, 2020. <https://www.un.org/en/universal-declaration-human-rights/>.

²²⁸ <https://unstats.un.org/unsd/statcom/51st-session/documents/2020-23-ICT-EE.pdf>.

²²⁹ “2020 Edelman Trust Barometer”. Edelman, 2020. <https://www.edelman.com/trustbarometer>.

Policy Makers

In addition to foreign and public policy experts, among those who must be included as policymakers for the future of internet policy are electrical engineers, computer scientists, mathematicians, and ICT logisticians. Journalists, economists, and programmers and those in the fields of cybersecurity, human rights, communications law, artificial intelligence, and grassroots development must also be included to ensure that these experts and policymakers avoid pushing the boundaries of freedom and security too far. Technical experts fluent in network and telecommunications management will ensure that technical aspects are accounted for in the decision-making process, minimizing the details that could be left out with dangerous consequences. This is critical, as these types of decisions highlight often missed issues when dealing with new ICT policy and will provide a foundation of what artificial intelligence methods can be used to uphold such policies. Mathematicians working in artificial intelligence have recently developed an algorithm using Benford's Law²³⁰ to track "bots" online and identify deep fakes²³¹. Misinformation is one of the major threats of the internet. The ability to enforce laws targeting misinformation by using this algorithm will be vital for ensuring that appropriate accounts and content are not removed, thus, lessening the potential for damage to internet freedom.

Recommendations

While the first drafts for the foundation of international internet law may fail to accurately determine the maximum and minimum amount of internet freedom for every nation, some matters must be included across the board with great attention to detail:

- the protection of journalists,
- right to criticize politicians,

²³⁰ Benford's Law is an observation about the frequency distribution of leading digits in many real-life sets of numerical data.

²³¹ Jennifer Golbeck. 2019. "Benford's Law Can Detect Malicious Social Bots". *First Monday* 24 (8). <https://doi.org/10.5210/fm.v24i8.10163>.

- individual data privacy,
- democratic/election interference,
- misinformation control and calls for violence.

Various experts and organizations must work in coordination to effectively and efficiently establish long lasting global ICT policy. Answers can be found by studying past and current examples of internet policy, the waves of globalization, and those who have a hand in internet operations. Globalization and the internet in relation to freedom and security is a complex topic, much of which was not covered in this article. However, a few recommended redlines based on what has been covered is provided.

The first priority is to prevent developed countries from turning away from globalism and the “Balkanization” of the internet. By doing so it avoids exacerbating human rights and creating other cybersecurity issues such as unequal access to information. Second, we must realize that there are ways to limit threats connected to the censorship of ourselves and other nations. Economic, social, geographical, historical, and cultural factors will be considered when establishing boundaries on the scope of internet regulation and censorship. Violating human rights and press freedom is where we must draw the line. The definition of “press” may need to be specified to make sure satire and false sources will not fall under this protection. Censorship and restrictions must be capped, and barriers to cross-border data flow removed, creating opportunities to benefit from and play a role in the global community made available to everyone. National internet policy will vary based on the factors listed above, but establishing international limits is necessary to ensure a minimum standard. One limit, for example, should be censoring criticism of public and political officials. Since the European Union’s recent decision on Directive 2000/31/EC stemmed from a disgruntled politician, the decision must be overturned to set an example and not an opportunity for corruption.

Third, citizens must hold their governments and stakeholders accountable for their actions and decisions, especially concerning user data privacy. International regulations should declare the use of data collection only when necessary, but the issue with this lies in what would be deemed

“unnecessary” and at what level would that decision be made. Again, the finer details would most likely have to be managed at the national level. Users should also be able to control who has access to their information and how it is used. Countries using E-governance, such as Estonia, utilize the Cloud for all bureaucratic purposes, including individual financial and medical documentation. Although this framework might not work for every country due to cybersecurity concerns, it is nevertheless something to aspire towards. Estonians have complete digital control of their information and no one has had any of their information stolen. The National Cyber Security Index ranks Estonia as the third most cybersecure nation and could be looked to for recommendations for secure networks²³². This will require a change in societal norms in many nations. There is a global shift in the opinion of democracy, with nearly all nations losing favor. The opinions in weaker democracies have changed twice as much as those in more democratic nations between 1998 and 2020. This coincides with the shift in levels of globalization as this opinion is exacerbated by the effects of the internet. For internet regulation policies to be adopted in a manner that benefits all, the opinions toward sacrificing some freedom for security must continue to be more acceptable²³³. At the same time, implementing these policies will require negotiations explaining that a path toward globalization is the only way to ensure long-term stability. We live in a world with infinite variations in ideals and morality, varying even within seemingly homogenous societies. Balancing social norms to lessen tensions over conflicting values over time might allow us to live peacefully.

Conclusion

A single government, social network, or person can take the blame for the state of the internet today. Energy is wasted on writing the narrative of how we got here and tracking these problems’ symptoms. Instead, we

²³² <https://ncsi.ega.ee/ncsi-index/>.

²³³ “A Rift in Democratic Attitudes Is Opening up around the World”. *The Economist*, August 22, 2020. <https://www.economist.com/graphic-detail/2020/08/22/a-rift-in-democratic-attitudes-is-opening-up-around-the-world>.

must focus on the root of what causes these problems and act in sync as a global internet community. Addressing this and the pattern of ICT effects on globalization is the only way to ensure long-term freedom and security. However, making these decisions civilly will not be an easy task as our world, even within homogenous societies, is unfathomably diverse regarding ethics, values, social norms, and expectations. Creating and implementing internet policy at the international level will require a case by case study, precise terminology, and means of enforcement. Cases of China, the European Union, and the United States have already been highlighted in this paper. However, least developed nations on both sides of the internet freedom index must be considered when experts and policymakers begin setting the foundation. Placing too many restrictions will limit the growth of globalization and exacerbate existing political tensions. On the other hand, failing to define terminology and details will offer corrupt leadership opportunities to hinder growth and exacerbate present tensions. Staying ahead of and stabilizing the wave of globalization with these recommendations in mind will ensure long-term security and protection of freedoms. No matter the approach, there needs to be action in the international community on internet regulations for the sake of international stability.

The American Ape at the CIA: The Origin of Evolved and Learned Cognitive Mechanisms that Cloud Intelligence Analysts' Reasoning

Steven DAVIC

Abstract: All human behavior may be understood as an interaction between genes and the environment. The integration of innate cognitive mechanisms (from genes) and learned cultural mindsets (from the environment) profoundly affects our ability to perceive and interact with the world around us rationally. While we share innate cognitive mechanisms across the human population, cultural mindsets have substantial variation, even within the same country. Both the innate cognitive mechanisms and learned cultural mindsets have a substantial influence on intelligence and security analysts' objective reasoning abilities. Challenges arise when analysts' cultural mindsets do not align with their targeted group's (or individual's) cultural mindsets. Although the Intelligence Community (IC) has made significant strides to address these challenges, through structured analytical techniques (SATs), the professionalization of intelligence analysis, and uniform analytical standards, insights from other academic disciplines may offer additional/alternative solutions. In this paper, knowledge from Evolutionary Psychology, Cultural Anthropology, and Neuroscience is explored to gain insight into why humans view the world in diverse but shared ways, and its implications on the intelligence community.

Keywords: Evolutionary psychology, structured analytic techniques, intelligence analysis, information analysis, intelligence services, cheater-detection

What is Intelligence Analysis?

Evolutionary and cultural forces engage with, influence, and shape analysts' views of the world. Before exploring the origins of these forces, it is crucial to understand the roles and responsibilities of analysts across the intelligence community. To this end, we will consider the common themes and considerable variation across some of the world's premier intelligence agencies. Only after understanding the definitions, processes, analysts, and agencies that make up the intelligence discipline, can we explore the evolutionary and cultural forces that shape them.

The Definitions

Finding a universally accepted definition of intelligence analysis (IA) is difficult. Some intelligence practitioners might say, there are an equal number of definitions for "intelligence analysis" as there are former and current intelligence analysts. This disparity is because defining intelligence analysis often depends on the definer's context and their relationship or role within the intelligence community. This variation is best shown through the definitions provided by the Central Intelligence Agency (CIA) and the RAND Corporation (a prominent think-tank in the United States).

The CIA is focused on national security and foreign policy concerns for the United States. This mission is reflected in the definition of intelligence analysis, posted on their website as *"the application of individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context."*²³⁴. Their internationally-focused and often classified missions are reflected in their definition of IA, hence their inclusion of *"secret socio-cultural context."*

A slightly different definition offered by RAND Corporation reflects RAND's past projects and current clients within the military community. RAND

²³⁴ Rob Johnson, "Analytical Culture in the U.S. Intelligence Community: An Ethnographic Study", Central Intelligence Agency (Central Intelligence Agency, June 28, 2008), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm, 4.

defines intelligence analysis as *“the process by which the information collected about an enemy is used to answer tactical questions about current operations or predict future behavior.”*²³⁵. RAND’s definition has a military focus, reflecting their role within the defense industry. Their role is shown through their operational control over four federally funded research and development centers (FFRDCs), in cooperation with the U.S. Army, U.S. Air Force, U.S. Department of Homeland Security, and U.S. Office of the Secretary of Defense²³⁶.

Our definition of IA will correspond to this paper’s focus – innate cognitive mechanisms and culturally learned mindsets. For the working definition, we will define **intelligence analysis** as *processing environmental data until it possesses an advantage for an entity operating within that environment*. This definition is an all-encompassing one, that does not unnecessarily constrain intelligence to mediums of collection, methods of analysis, customers of products, or scope and context of functional value. Furthermore, it presents the contemporary structure and goal of intelligence analysis as an attempt to expand and refine reasoning abilities that are naturally evolved and purposely cultivated within all humans.

The Processes

Similar to defining intelligence analysis, conducting intelligence analysis is done through different processes depending on the mission and its desired outcome. Despite these differences, the foundational steps for intelligence analysis are relatively similar across all applications. Dr. Noel Hendrickson, the founder of the Intelligence Analysis program at James Madison University (JMU), describes the general process in his book *Reasoning for Intelligence Analysis*²³⁷. Hendrickson explains the four steps as the following.

²³⁵ “Intelligence Analysis”, RAND Corporation, accessed August 18, 2020, <https://www.rand.org/topics/intelligence-analysis.html>.

²³⁶ “RAND Federally Funded Research and Development Centers (FFRDCs)”, RAND Corporation, accessed August 18, 2020, <https://www.rand.org/about/ffrdc.html>.

²³⁷ Noel Hendrickson, *Reasoning for Intelligence Analysis: A Multidimensional Approach of Traits, Techniques, and Targets* (New York City, NY: Rowan and Littlefield, 2018), 26–27.

1. “Search and collect” to generate data to analyze.
2. “Represent and structure” the data into meaningful information.
3. “Evaluate and infer” knowledge in the context of its relation to the truth.
4. “Disseminate and use” the inference in a practical way for the client.

Because Dr. Hendrickson has an educator’s role within the IC, his definition of the intelligence process is an analyst-centered one, concerned with developing students into junior analysts. Other versions account for an “administrative step” before an analyst begins searching and collecting information. Katherine and Randolph Pherson – widely regarded in the intelligence community for their contributions towards standardizing the intelligence discipline, present in their book *Critical Thinking for Strategic Intelligence*, a version of the intelligence cycle widely used by the U.S. and Canadian government. Their version includes the additional administrative step²³⁸. The five steps are:

1. Planning, Direction, Needs, and Requirements
2. Collection
3. Processing and Exploitation
4. Analysis
5. Dissemination

In addition to the added step, Pherson and Pherson describe the intelligence process as a cycle²³⁹. Once intelligence assessments are disseminated, analytical judgments are used to inform future planning, direction, needs, and requirements. This workflow restarts the process, creating a continuous intelligence cycle. Regardless of how many steps are included within the intelligence process (or cycle), each step is critical to producing relevant, accurate, and timely intelligence.

²³⁸ Katherine Pherson and Randolph Pherson, *Critical Thinking for Strategic Intelligence*, 2nd ed. (Thousand Oaks, CA: CQ Press, 2017), 89.

²³⁹ Pherson, *Critical Thinking*, 89.

The Analysts

While the IA discipline has become increasingly aided by artificial intelligence and data analytical tools, at its very core is a human-centered field. Because humans are fallible, their created processes and expressed behaviors follow suit. Humans add this imperfect dynamic to the intelligence cycle, which creates ambiguity and inaccuracies. Because of the imperfect nature of humans (and in turn analysts), it is important to understand different positions and roles analysts take on within the intelligence cycle, especially in search of the origins of past intelligence shortcomings. While analysts are not the only cause of intelligence shortcomings, they certainly play a large role.

Roles of Analysts

As a community, analysts conduct intelligence analysis across multiple mediums, on vastly different subjects, and for many clients. As a result, they are required to perceive, analyze, and assess a range of topics. Because of this diversity, the roles and desired technical skills recruited for, greatly vary among agencies.

Most analysts within the community, are concentrated on specific elements of the intelligence cycles defined above. Because of their specific focuses, roles for intelligence analysts range from technical jobs in cybersecurity and satellite imaging, to human-centered jobs like interrogators and linguists, to dissemination-focused jobs like multimedia producers and technical writers, to other various subject matter expertise ranging from nuclear physics to aerospace engineering²⁴⁰.

As we will see in the following sections, academic background and technical skills are not the only things that distinguish analysts. Experiences ranging back to their first years, including childrearing techniques in infancy and parenting-styles during childhood, have significant influences on

²⁴⁰ "Careers & Internships: Browse Jobs by Category", Central Intelligence Agency (Central Intelligence Agency, December 12, 2019), <https://www.cia.gov/careers/opportunities/cia-jobs/index.html>.

analysts' variability in reasoning, perception, and judgment²⁴¹. However, despite the vast array of roles, expertise, and influences an analyst can have, there is a shared suite of traits that is cross-culturally agreed upon to be beneficial for analysts to possess.

Traits of Analysts

Regardless of roles, analysts are charged with taking an independent and objective-based perspective on issues, free from pressure to “prove” or “support” a given worldview or hypothesis. Because of this uniform goal, the suite of traits that are recruited for and trained towards across all intelligence agencies are rather similar. Dr. Hendrickson encapsulates this suite of traits into four “sought-after” characteristics of analysts²⁴².

1. Intellectual Courage – *summarized as balancing confidence vs. uncertainty, neutrality vs. real-world concern, and breadth vs. depth of inquisitive knowledge.*
2. Intellectual Self-Control – *summarized as balancing sensitivity towards similarity vs. change, thoroughness vs. expediency, and descriptive quality vs. quantity.*
3. Discernment – *summarized as reflectiveness on self vs. other, versatility between spontaneity and deliberateness, and integration of “bottom up” vs. “top-down” approaches of thought.*
4. Intellectual Fairness – *summarized as recognizing threats vs. opportunities, conveying specificity vs. simplicity, and reflecting objections vs. refinements.*

These characteristics, or “cognitive virtues” as Hendrickson calls them, help analysts provide an independent and objective analytical stance on incoming information. However, these traits are difficult to gain and maintain by even the most disciplined analysts. As we will explore in later sections, our evolutionary past and specific cultural upbringing have much to do with this.

²⁴¹ Michael Harris Bond, *The Oxford Handbook of Chinese Psychology* (Oxford, UK: Oxford University Press, 2015), 32–67.

²⁴² Hendrickson, *Reasoning*, 72–82.

The Agencies

Analysts are regularly recruited based on an agency's specific mission and home country's unique challenges. Additionally, Dr. Timothy Walton – a senior CIA analyst and Kent School instructor turned university professor – notes, how intelligence agencies often reflect the cultural values within a particular country²⁴³. This assertion is supported by other intelligence reformers²⁴⁴ and is reflected in recent job postings for analysts in the United States' CIA and Japan's Public Security Intelligence Agency (PSIA)^{245, 246}.

U.S. vs. Japanese Intelligence Recruitment

The CIA is charged with collecting and assessing foreign intelligence, relying heavily on foreign language skills. Because only 20% of American K-12 students enroll in foreign language classes (compared to 92% in the European Union), many CIA job postings place an emphasis and premium on foreign language skills and international travel²⁴⁷. The premium placed on foreign language skills shows how American culture and current challenges are reflected in CIA job postings.

In another example, the application for the PSIA reflects a wider cultural emphasis and reliance on standardized testing. The Japanese education system places extraordinary pressure on high school students to score good grades on entrance exams to enter college^{248, 249}. This reliance on exams is at the forefront of assessing intelligence candidates. The PSIA demands

²⁴³ Timothy Walton, Lecture at James Madison University, March 23, 2020.

²⁴⁴ Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 8th ed. (Thousand Oaks, CA: SAGE/CQ Press, 2020), 441–499.

²⁴⁵ Central Intelligence Agency, "Careers & Internships".

²⁴⁶ "About the PSIA", PSIA | 公安調査庁 (Public Security Intelligence Agency, 2020), <http://www.moj.go.jp/psia/English.html>.

²⁴⁷ Kat Devlin, "Unlike in US, Most European Students Learn a Foreign Language", Pew Research Center (Pew Research Center, August 6, 2018), <https://www.pewresearch.org/fact-tank/2018/08/06/most-european-students-are-learning-a-foreign-language-in-school-while-americans-lag/>.

²⁴⁸ Yoshitaka Saito. "Consequences of high stakes testing on the family and schools in Japan". *KEDI Journal of Educational Policy* 3, no. 1 (2006).

²⁴⁹ Kathleen Kitao and Kenji Kitao, *An Analysis of Japanese University Entrance Exams Using Corpus-Based Tools*, 2008, <http://www.j-let.org/~wcf/proceedings/d-053.pdf>.

candidates to pass the “National Civil Service Recruitment Comprehensive Employment Exam” before being considered for an interview²⁵⁰. This emphasized importance on exams is heightened by customary “lifetime” employment once selected, an absence of an initial probationary period, and a low degree of lateral mobility once hired²⁵¹. These Japanese cultural norms surrounding its PSIA and civil service increase the selectivity and reliance on a standardized examination.

Unique Challenges and Threats

As many intelligence practitioners point out, agencies are often formed as a reactive need to a past problem. This trend is shown in the presidential directives that established the Office of Strategic Services, National Security Agency, and Homeland Security Agency within the United States.²⁵² Once created, the focus and organizational structure of these newly formed agencies, reflect the current threats and challenges being faced by that nation. Outside of the United States, this reflection is seen in Chinese, French, and Japanese intelligence agencies.

China’s recent economic expansion and regional security issues guide their intelligence agency’s efforts. Chinese espionage appears to be focused on four primary targets: economic data, military equipment, reconnaissance of critical infrastructure, and attacks on critics²⁵³. This focus reflects their national strategy of maintaining remarkable economic growth²⁵⁴, updating their military into a modern superpower²⁵⁵, conducting widespread

²⁵⁰ “Career Track Recruitment”, Public Security Intelligence Agency (Public Security Intelligence Agency, 2020), <http://www.moj.go.jp/psia/sougou.html>.

²⁵¹ Byung Chul Koh. “The Recruitment of Higher Civil Servants in Japan: A Comparative Perspective”. *Asian Survey* 25, no. 3 (1985): 292–309. Accessed August 18, 2020. doi:10.2307/2644120.

²⁵² “What Was OSS?” Central Intelligence Agency. Central Intelligence Agency, June 28, 2008. <https://www.cia.gov/library/publications/intelligence-history/oss/art03.htm>.

²⁵³ Lowenthal, *Intelligence*, 454.

²⁵⁴ Xing-Ping Zhang, and Xiao-Mei Cheng. “Energy consumption, carbon emissions, and economic growth in China”. *Ecological Economics* 68, no. 10 (2009): 2706–2712.

²⁵⁵ Elsa Kania. “Innovation in the New Era of Chinese Military Power”. *The Diplomat*. The Diplomat, July 25, 2019. <https://thediplomat.com/2019/07/innovation-in-the-new-era-of-chinese-military-power/>.

infrastructure projects (both domestically and internationally)²⁵⁶, and guarding their political image against dissidents²⁵⁷.

Because of recent terrorist attacks, France now puts a significant intelligence emphasis on terrorism. In 2012, a lone-wolf terrorist attack killed seven people; this attack was followed in 2015 with ISIL-backed terrorist attacks in Paris, killing over 100 people and injuring over 350²⁵⁸. Additionally, because France is one of several nuclear-weapons powers of Europe, it remains concerned about the development and proliferation of Weapons of Mass Destruction (WMDs). One government official estimated half of intelligence activity is devoted to WMDs and counterterrorism²⁵⁹. Presently, these two concerns are the regional issues that guide France's intelligence efforts.

Japan is restricted within their military and intelligence community, because of limitations imposed following World War II²⁶⁰. This limitation, along with their dynamic and threatening regional neighbors, has compelled Japan to maintain a regional (rather than global) focus on the intelligence efforts. Their consistent monitoring of China and North Korea, along with security sharing agreements between South Korea and Australia, reflect Japan's emphasis on regional concerns²⁶¹.

As demonstrated, a country's intelligence agencies reflect their current and anticipated threats, national culture, and tasked mission. Despite these differences, most agencies share similar overall missions: to provide accurate and timely intelligence to decision-makers. However, the inflow

²⁵⁶ Sarker, Md Nazirul Islam, Md Altab Hossin, Xiaohua Yin, and Md Kamruzzaman Sarker. "One Belt One Road initiative of China: Implication for future of global development". *Modern Economy* 9, no. 4 (2018): 623–638.

²⁵⁷ Danny O'Brien. "China's Global Reach: Surveillance and Censorship Beyond the Great Firewall". Electronic Frontier Foundation, December 29, 2019. <https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall>.

²⁵⁸ Lowenthal, *Intelligence*, 458.

²⁵⁹ Ibid, 459.

²⁶⁰ Lee Hudson Teslik,. "Japan and Its Military". Council on Foreign Relations. Council on Foreign Relations, April 13, 2006. <https://www.cfr.org/background/japan-and-its-military>.

²⁶¹ Lowenthal, *Intelligence*, 493.

of information in today's "Information Age" makes this mission increasingly challenging. To counter this, agencies use various techniques, called Structured Analytical Techniques (SATs) to help analysts conduct their assessments.

The Techniques

Intelligence Analysts use structured analytical techniques (SATs) to "*challenge judgments, identify mental mindsets, stimulate creativity, and manage uncertainty*."²⁶² They were created and standardized in response to a long history of intelligence failures. While this is certainly not an exhaustive list, the CIA's Tradecraft Primer lists these techniques in three basic categories²⁶³.

First, diagnostic techniques are primarily *focused on making the methodology transparent, that was used to arrive at an assessment*. Examples include Key Assumptions Check, Quality of Information Check, Indicators or Signposts of Change, and Analysis of Competing Hypotheses (ACH)²⁶⁴. One example of how these techniques could have been useful is in the case of the 2002 DC sniper. In the fall of 2002, an onset of sniper attacks occurred in the Washington DC region. Law enforcement quickly made a set of assumptions about the sniper: it was a lone white male with military training driving a white van²⁶⁵. By conducting a **Key Assumptions Check**, analysts could have *challenged the assumptions*, remained receptive to all leads (including reports of the sniper fleeing in a Chevrolet car). Further investigations and arrests found the sniper to be a team of black males driving a car – far from the initial assumptions.

Next, contrarian techniques are primarily *used to provide alternatives to current assessments*. Examples include Devil's Advocacy, Team A/Team B,

²⁶² A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis (Washington, DC: U.S. Government, 2009), <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf>.

²⁶³ Ibid.

²⁶⁴ Ibid.

²⁶⁵ CIA, *Tradecraft*, 8.

High-Impact/Low-Probability Analysis, and “What if?” Analysis²⁶⁶. Intelligence shortcomings revolving around the Pearl Harbor attack could have benefited from all three techniques listed above. By forming a devil’s advocacy team, or *group of analysts to challenge the consensus belief* surrounding Pearl Harbor (the Japanese would not attack), the government could have outlined possible reasons for the Japanese to initiate an attack.

Finally, imaginative thinking techniques are primarily *aimed at moving analysts out of fixed mindsets to develop new insights and perspectives*. Examples include Brainstorming, Outside-In Thinking, Red Team Analysis, and Alternative Futures Analysis²⁶⁷. Again, preceding the attack on Pearl Harbor, analyst could have conducted a Red Team analysis, or *looked at the situation from the adversary’s perspective*. Doing this would have shown a formidable United States, quickly gaining strength while building up their military-industrial base. An imminent attack would have provided any hope in crushing the United State’s Pacific fleet and will to fight.

The previous section shared a collection of some of the main SATs used within intelligence agencies. As demonstrated, many of these techniques are applicable to the same situation and can be used in conjunction with each other. While the scope of this paper does not intensely focus on the individual techniques, it is important to note the main purpose of creating and standardizing them: to counter evolved and learned mindsets of analysts.

Intelligence Analysis: summary

Understanding the different definitions of Intelligence Analysis, variations in the missions of intelligence agencies, and the diverse roles intelligence analysts carry out is critical. However, seeing the commonality across all agencies and countries through shared missions and challenges is equally important. In this paper, I presented a brief overview of the definitions, processes, analysts, and agencies that make up the Intelligence

²⁶⁶ Ibid.

²⁶⁷ Ibid.

Community. We explored the common themes across all agencies and the diverse influences that creates unique variations among them. We will use this foundational overview to examine the evolutionary and cultural forces that engage with, influence, and shape analysts' views of the world.

Evolved Cognitive Mechanisms

Many questions about our species origins remain unanswered today. Each year archaeologists, anthropologists, and geologists uncover more clues into how modern humans evolved from past ancestors. Despite these unanswered questions, the Theory of Evolution is one of the most established and scientifically supported theories across modern science – below we explore some of its themes. First, we attempt to condense the theories which describe millions of years of evolution into a few pages. After, we will use this brief overview to help explain the current cognitive mechanisms and processes within analysts' brains. While the evolved cognitive mechanisms explored below are present in all of us, some readers may find them invisible or nonexistent within their own minds.

Evolution of the Human Body

The theory of evolution describes how all life has evolved and, of relevance, how humans evolved into our modern form over the last 200,000 years²⁶⁸. The theory describes how changes in heritable traits that increase the **fitness level** of an individual, or *ability to survive and reproduce*, slowly spread throughout a population. These changes are often brought on by a **selection pressure**, or *an agent that affects survival and reproduction within a species*²⁶⁹. When *a trait, that increases the individual's fitness, is selected for and gains prevalence in a population*, it is known as an **adapt-**

²⁶⁸ Daniel E., Lieberman, Brandeis M. McBratney, and Gail Krovitz. "The evolution and development of cranial form in Homo sapiens". *Proceedings of the National Academy of Sciences* 99, no. 3 (2002): 1134–1139.

²⁶⁹ Joel S. Brown, John W. Laundre, and Mahesh Gurung. "The Ecology of Fear: Optimal Foraging, Game Theory, and Trophic Interactions". *Journal of Mammalogy* 80, no. 2 (1999): 385–99. Accessed August 23, 2020. doi:10.2307/1383287.

tion. For example, **bipedalism**, or *the ability to walk on two legs*, is an evolved trait (adaptation) caused by either selection pressures related to environmental changes (e.g., aridification of the habitat that leads to fewer forests), or social changes (e.g., walking on two legs instead of four frees up the hands to carry food or infants)²⁷⁰. Whatever the specific selection pressures are that led to the evolution of bipedal walking, **hominins**, or *bipedal ape-like ancestors of the human species*, who evolved slightly more arched feet, curved spines, and wider hips, had an easier time balancing and walking on two feet²⁷¹. This adaptation helped them to save calories (which were increasingly more difficult to obtain)²⁷². Those who possessed these advantageous traits out-survived and out-reproduced those who had inferior versions of these traits. As a result, more of the next generation possessed these traits. This change continued until the collective advantage (of arched feet, curved spines, and wider hips) became more refined and increased in frequency across the entire population. Once bipedality had evolved, selection pressures continued to act on the human skeleton to make bipedal walking more efficient.

Much like physical traits, such as bone/muscle changes for efficient bipedal walking, humans also evolved cognitive traits, which similarly presented an adaptive advantage for those who possessed them. The evolution and dissemination of these traits happened much like those of our physical adaptations: individuals possessing a beneficial cognitive mechanism out-survived and out-reproduced those that did not have that mechanism.

Evolution of Cognition

Evidence suggests that two mechanisms influence human cognition and behavior: the instincts we inherit through genes, and the “cultural download” of information we learn through social interactions²⁷³.

²⁷⁰ Daniel E. Lieberman, *The Story of the Human Body: Evolution, Health, and Disease* (New York City, NY: Vintage Books, 2013), 25–48.

²⁷¹ Ibid.

²⁷² Ibid., 42.

²⁷³ Peter J. Richerson, Robert Boyd, and Joseph Henrich. “Gene-culture coevolution in the age of genomics”. *Proceedings of the National Academy of Sciences* 107, no. Supplement 2 (2010): 8985–8992.

More so than any other species, humans have a collection of innate cognitive mechanisms that are used to survive in our environment – evolutionary psychology studies these mechanisms. Charles Darwin, “the father of evolution”, foresaw the emergence of this discipline. Towards the end of *Origin of Species*, he envisions the field of psychology expanding towards new research areas that sought to understand the design and adaptations that led to the modern human minds²⁷⁴. Decades later, William James released a groundbreaking piece of work titled *Principles of Psychology*, that began to explore this, choosing to focus heavily on **instincts**, or *specialized, innate, neural circuits, present across a species, that emerged as a product of evolution*²⁷⁵. At the time, it was commonly understood that animals were mostly guided by instincts (and had many of them), while humans were mostly guided by reason (and had fewer instincts). Furthermore, scientists believed the lower amount of human instincts allowed humans to be “more flexibly intelligent than other animals.”²⁷⁶. James countered this by arguing that humans had higher “flexible intelligence” because we had more instincts²⁷⁷. These instincts function efficiently and effortlessly (by collecting environmental stimuli, processing information, and guiding behavior) that we are “blind” to their existence. Years later, advancements in genetics, biology, neuroscience, and psychology have universally and unequivocally supported that instincts are shared cross-culturally across all of humanity²⁷⁸. However, the idea that they solely guide our behavior and account for our “flexible intelligence” is highly disputed. As we will learn in later sections, cultural and social influences play a significant role in our intelligence superiority over our primate relatives.

²⁷⁴ Charles Darwin. *On the Origin of Species*. www.gutenberg.org. 6th ed. Accessed August 18, 2020. <http://www.gutenberg.org/files/2009/2009-h/2009-h.htm>.

²⁷⁵ William James. *The Principles of Psychology*. Vol. 1. Cosimo, Inc., 2007.

²⁷⁶ Leda Cosmides and John Tooby. “Evolutionary psychology: A primer”. (1997).

²⁷⁷ James William, *Principles*.

²⁷⁸ Robert Boyd and Peter J. Richerson. “Culture and the evolution of the human social instincts”. *Roots of human sociality* (2006): 453–477.

Evolution of Environments

As we covered, innate cognitive mechanisms play a critical role in our cognitive success. However, they play an equally detrimental role in our cognitive errors and failures. These failures or misalignments are a result, in part, by our rapidly changing environment.

The modern environment we live in is extraordinarily different from the **Environment of Evolutionary Adaptedness (EEA)**, or *the past environment our species adapted to*. Hunting and gathering account for most of our evolutionary past, with groups traveling 5–15 kilometers a day to gather food²⁷⁹. Among many factors, predators, hostile groups, natural disasters, and lack of modern medicine made the past environment a harsh and formidable place. As we learned, humans evolved biological and psychological solutions to these adaptive problems.

However, a peculiar trait of the environment is that it changes much more rapidly than the speed of adaptation. This is because the rate of adaptation is set by the generation time of the species – for humans, the generation time is 22–33 years²⁸⁰. Demonstrated through the evolution of bipedalism, it could take tens of thousands of generations for an adaptation to gain prevalence in a population. As a result of this timeline, we still carry the same biological and psychological adaptations we evolved to solve the EEA challenges. Many of these adaptations we evolved in the past, such as attraction to sugar²⁸¹, and aversion to strangers²⁸², may now have lost their advantages or even present a disadvantage in this new environment. As we will see, these disadvantages encompass some of the gaps in logic and flawed reasoning that taint analysts' assessments today.

²⁷⁹ Lieberman, *The Story*, 42.

²⁸⁰ Ansley Johnson Coale. *Growth and Structure of Human Populations: A Mathematical Investigation*. Princeton University Press, 2015.

²⁸¹ Satyawhan Damle. "Smart sugar? The sugar conspiracy". *Contemporary Clinical Dentistry* 8, no. 2 (2017): 191–191.

²⁸² Jennifer Hahn-Holbrook, Colin Holbrook, and Jesse Bering. "Snakes, spiders, strangers: How the evolved fear of strangers may misdirect efforts to protect children from harm". *Protecting children from violence: Evidence-based interventions* 26 (2010): 3–289.

Impacts on the Intelligence Community

The misalignments of our evolutionary past and present cognition have contributed to intelligence shortcomings since the creating of intelligence agencies. The CIA's Tradecraft Primer attempts to categorize these misalignments into four categories of perceptual and cognitive biases²⁸³.

1. Perceptual Biases – we tend to perceive what we expect, resist change (even in the face of notable counter-evidence), and ambiguous information disproportionately interferes with correct judgments of a situation.
2. Biases in Evaluating Evidence – we do not immediately change our perception in light of discrediting information, we have more confidence in concluding small bodies of data that are consistent rather than large bodies of data with less consistency, and we have difficulty judging the potential impact of missing information.
3. Biases in Estimating Probabilities – people are often overconfident, unimaginative, and inconsistent when judging probabilities of an event in light of new evidence.
4. Biases in Perceiving Causality – people attempt to fit events into a perceived linear pattern of causality, often discrediting randomness and accidents.

The publication continues to cite these biases as the reason leading to recent intelligence failures including analysts over-connecting WMD but also under-connecting the evidence leading up to 9/11, over-estimating the spread of democracy after the Arab-Spring but under-estimating the response of Russia in Crimea, over-rating the Iraqi Army's ability in recent conflicts, but under-rating the strength of ISIS, and many others²⁸⁴. These biases have remained in the spotlight of intelligence agencies since their inception, as efforts are undertaken to counter them.

After the recent intelligence shortcomings around the 9/11 terrorist attacks and WMD programs in Iraq, congressional oversight committees

²⁸³ CIA, *Tradecraft Primer*, 2.

²⁸⁴ CIA, *Tradecraft Primer*, 2.

demanding the intelligence community (IC) become professionalized and standardized across all 17 agencies through added training and education opportunities, directives outlining analytical standards, and an emphasis on SATs. Additions to education across the IC, such as the CIA University, College of Analytical Studies, and National Intelligence University, attempted to do this²⁸⁵. Supporting directives, such as ICD 203, were released in an effort to institutionalize the roles, responsibilities, and analytical standards expected from intelligence analysts²⁸⁶. Later publications, such as the CIA's Tradecraft Primer, were publicized and distributed to normalize SATs²⁸⁷. Indeed, in the past two decades, great strides have been made in improving intelligence analysis efforts.

Despite these changes to the IC, intelligence practitioners such as Dr. Stephen Marrin, renowned for his work in intelligence reform and education, call for further improvements while questioning past ones. Dr. Marrin explores in several published essays whether SATs work better than intuition^{288, 289}. He proposes, among many things, that more time, energy, and resources be devoted to evaluating their accuracy and utility towards real-world applications.²⁹⁰ In other publications, he scrutinizes the fast-paced and continuous nature of intelligence production. He argues the IC places undue emphasis on short-term, daily intelligence briefings, rather than long-term, prospective, deep-analysis of a topic²⁹¹. This focus inhibits analysts' ability to develop the foundational and topical expertise required to make sound judgments. I propose that this may increase the reliance on structured analytical techniques to do the "thinking" and "analysis" for intelligence professionals, since they have not developed enough "topical

²⁸⁵ Stephen Marrin, "Training and Educating U.S. Intelligence Analysts", *International Journal of Intelligence and CounterIntelligence* 22, no. 1 (November 2008): pp. 131–146, <https://doi.org/10.1080/08850600802486986>.

²⁸⁶ Intelligence Community Directive 203 (2015).

²⁸⁷ CIA, *Tradecraft Primer*.

²⁸⁸ Marrin, *Training and Educating*.

²⁸⁹ Stephen Marrin. "Intelligence Analysis: Structured Methods or Intuition?" *American Intelligence Journal* 25, no. 1 (2007): 7–16. Accessed August 18, 2020. www.jstor.org/stable/44327067.

²⁹⁰ Marrin, *Training and Educating*.

²⁹¹ Ibid.

expertise.” Although the effectiveness of certain SATs is not agreed upon or established, SATs have been offered as a solution to counter the intuitive mindsets of analysts.

Evolved Cognitive Mechanisms: the summary

These new insights show that humans possess a vast collection of instincts that broadly guide our attention, influence our thinking, and regulate our behavior. These instincts, or innate cognitive mechanisms, create biases in our thoughts, inconsistencies in our judgments, and inaccuracies in our perceptions. However, while our evolutionary past plays a large role in guiding our current mindsets and behaviors, it does not play the only role. In the next section, we will explore the second influence on human cognition – the “cultural download” received from birth into adulthood.

Learned Cognitive Mindsets

The innate cognitive mechanisms undoubtedly help lead to our success as a species – but they’re not the complete solution. For example, imagine a stockbroker from Wall Street, born and raised in the city, was placed into the Amazonian rain forest. There are no instinctual modules that “fire up” to help him find food, make fire, or build a shelter – yet humans have survived in the Amazon Basin for thousands of years²⁹². He is missing, what Dr. Joseph Henrich (an evolutionary biologist at Harvard) describes as, a “cultural download” of knowledge (in this case, knowledge on how to survive in the jungle.)²⁹³ In his book, *The Secret of Our Success*, he describes the “flexible intelligence” (previously talked about) as not coming from our instincts but being socially learned and passed down from one generation to the next. These social connections and cultural institutions, he argues,

²⁹² Jonas Gregorio De Souza, Denise Pahl Schaan, Mark Robinson, Antonia Damasceno Barbosa, Luiz E. O. C. Aragão, Ben Hur Marimon, Beatriz Schwantes Marimon, et al. “Pre-Columbian Earth-Builders Settled along the Entire Southern Rim of the Amazon”. *Nature Communications* 9, no. 1 (2018). <https://doi.org/10.1038/s41467-018-03510-7>.

²⁹³ Joseph Patrick Henrich, *The Secret of Our Success: How Culture Is Driving Human Evolution, Domesticating Our Species, and Making Us Smarter* (Princeton, NJ: Princeton University Press, 2016).

have allowed us to produce sophisticated technologies, complex languages, and an ever-growing body of knowledge.

Defining Culture

Humans, within a specific environment, faced many of the same challenges. These shared challenges led to a similarly shared collection of solutions used to solve these challenges. Many of these shared solutions take the form of cultural norms such as languages, numbering systems, spices in cuisine, and building styles. From this stance, we define **culture** as *a set of shared experiences*. Because of this broad definition, culture is not limited to ethnicity, religion, or geographies, as some definitions often restrict it to. Instead, it encompasses the shared behaviors, mindsets, and perspectives that are passed down through means other than genetics²⁹⁴. Cultures range across all domains of life, including hobbies, sports, hometowns, countries, religions, ethnicities, academic degrees, and much more. Since humans participate in many of these experiences, we can say that humans are the sum of many different cultures. Before understanding the influence of these cultures on our cognition, we must conduct an overview of our brain and its ability to be influenced by experience (and culture) – to that end, we continue.

Early Brain Development

Our brain is constructed by more than 86 billion nerve cells²⁹⁵, connected in functional networks and pathways, all with specific jobs²⁹⁶. These *functional networks of neurons*, or **neural circuits**, are created during prenatal development and guided by **genes**, or *life-building instructions within our chromosomes*²⁹⁷. Genes specify how the body and brain are assembled

²⁹⁴ Robert Sapolsky, *Behave: The Biology of Humans at Our Best and Worst* (London, UK: Penguin Random House, 2017), 271.

²⁹⁵ Suzana Herculano-Houzel. "The human brain in numbers: a linearly scaled-up primate brain". *Frontiers in human neuroscience* (2009): 31.

²⁹⁶ Department of Biochemistry and Molecular Biophysics Thomas Jessell, Steven Siegelbaum, and A.J. Hudspeth. *Principles of neural science*. Edited by Eric R. Kandel, James H. Schwartz, and Thomas M. Jessell. Vol. 4. New York: McGraw-hill, 2000.

²⁹⁷ Ibid.

during development²⁹⁸. These genes are inherited from our parents, and immediately begin building a brain capable of learning. Simply put, **learning** is *external stimuli strengthening or weakening existing pathways, in anticipation of future usage*. At the earliest stages of life, during prenatal development, these circuits and pathways immediately began being used (and not used), subsequently becoming more strongly (or weakly) connected²⁹⁹. This concept is known as **Hebbian theory**³⁰⁰, which states *the connections between two neurons are strengthened through repeated firing*. As we grow older, the *ability for our neural connections to change in response to environmental stimuli*, or **neural plasticity**, weakens. This term explains why children generally have an easier time learning languages and new skills³⁰¹. Because of the tremendous amount of neural plasticity in children's brains, the events and environments they encounter profoundly impact their brain development³⁰². This early usage of neural networks (or lack of) dramatically affects our neural connections, and consequently, how we process information and the world around us.

All behavior is guided by the interaction between genes and the environment³⁰³. To this end, two things determine the usage and subsequent strengthening and weakening of all neural pathways. First, genes create and assemble the brain into specialized modules. The second way the usage of these pathways is determined is through external environmental information input through the senses. Each human inherits a unique "starting point" of neural pathways (from their parent's genes), as well as a unique "cultural download" from their parents and the surrounding environment. As previously mentioned, prominent anthropologists such as Dr. Henrich,

²⁹⁸ Ibid.

²⁹⁹ Donald Olding Hebb. *The organization of behavior: a neuropsychological theory*. J. Wiley; Chapman & Hall, 1949.

³⁰⁰ Ibid.

³⁰¹ Heidi C Dulay and Marina K. Burt. "Natural sequences in child second language acquisition 1". *Language learning* 24, no. 1 (1974): 37–53.

³⁰² J.P. Mersky, J. Topitzes, and Arthur J. Reynolds. "Impacts of adverse childhood experiences on health, mental health, and substance use in early adulthood: A cohort study of an urban, minority sample in the US". *Child abuse & neglect* 37, no. 11 (2013): 917–925.

³⁰³ Jessell, *Principles*.

suggest this cultural download is the secret to our flexible intelligence (or as he puts it in the title of his book *The Secrets of Our Success*.) We know that even these earliest changes and manipulation of neural pathways have fundamental and foundational implications towards learning³⁰⁴, temperament³⁰⁵, socialization³⁰⁶, and perception of the world³⁰⁷.

Shared Brain Development

These earliest influences, known to be “relative, conditional, and changeable”, are ultimately dependent on the environment of development³⁰⁸. However, shared experiences within a circumscribed social group or population are shown to produce similar effects on cognition and emotion; simply put, different cultures can have different shared experiences and thus different cognitive biases³⁰⁹. These psychological similarities within cultural groups are developed in the first months of infancy³¹⁰. Shared cultural norms and current geopolitical events that guide parenting techniques and childrearing styles can become distinct from other cultures, leading to cultural diversity. This is in part because culturally common parenting styles result in similar environmental stimuli introduced to children, resulting in similar neural network manipulations³¹¹. The related effects on neural networks result in children collecting and processing information (cognition), as well as behaving and expressing emotions in similar ways within a culture. Because socioeconomic and cultural factors determine

³⁰⁴ Bond, *The Oxford*, 32–67.

³⁰⁵ Ibid.

³⁰⁶ Ibid.

³⁰⁷ Ibid.

³⁰⁸ Fan, L. “On contradiction in cognition development: A personal view”. In *Issues in cognition: Proceedings of a joint conference in psychology*. Washington, DC: National Academy of Sciences, American Psychological Association. 1984.

³⁰⁹ Sapolsky, *Behave*, 266–302.

³¹⁰ Ibid.

³¹¹ Chen, Xinyin, Janet Chung, Rachel Lechcier-Kimel, and Doran French. “Culture and Social Development”. *The Wiley-Blackwell Handbook of Childhood Social Development*, 2011, 141–60. <https://doi.org/10.1002/9781444390933.ch8>.

parenting and childrearing techniques³¹² it is safe to say an individual's ecological environment, including language, culture, education, social class, etc., plays a critical and significant role in accounting for differences in cognition between cultures³¹³.

Many theories explore cultural effects on human development. According to Bronfenbrenner's ecological theory, the beliefs, values, and practices of culture play a significant role in lifetime development³¹⁴. Other theories concentrate on the indirect consequences of culture by viewing the social institutions, education systems, and community services that culture constructs to affect development^{315, 316}. Still, other theories look at the transmission and internalization of language and its effect on early childhood development^{317, 318}. Language may have a profound impact on cognition because of its immediate focus to learn, constant exposure, and use for mental processes in practically all cognitive tasks³¹⁹. As these studies suggest, by simply varying the language in which an analyst speaks, perceptions of the same event or information may differ similarly – other variations among analysts are likely to cause related effects on perception.

³¹² Marc H. Bornstein, "Cultural Approaches to Parenting". *Parenting* 12, no. 2–3 (2012): 212–21, <https://doi.org/10.1080/15295192.2012.683359>.

³¹³ Antonio E Puente, Maria Sol Mora, and Juan Manuel Munoz-Cespedes, "Neuropsychological assessment of Spanish-speaking children and youth", In *Handbook of clinical child neuropsychology*, pp. 371–383. Springer, Boston, MA, 1997.

³¹⁴ Urie Bronfenbrenner, Pamela A. Morris, William Damon, and Richard M. Lerner, "Handbook of child psychology", *The ecology of developmental process*. Wiley Publishers (2006).

³¹⁵ Ibid.

³¹⁶ Charles M. Super, and Sara Harkness, "The developmental niche: A conceptualization at the interface of child and culture", *International journal of behavioral development* 9, no. 4 (1986): 545–569.

³¹⁷ Barbara Rogoff, *The cultural nature of human development*, Oxford university press, 2003.

³¹⁸ Lev Vygotsky, "Interaction between learning and development", *Readings on the development of children* 23, no. 3 (1978): 34–41.

³¹⁹ Alexander V. Kravchenko, "How Humberto Maturana's biology of cognition can revive the language sciences", *Constructivist Foundations* 6, no. 3 (2011): 352–362.

Mental Maps of Reality

Apart from behavioral differences, culture also affects the way we experience the world around us. This component of culture is known as **mental maps of reality (or mental mindsets)**, which act as *cognitive templates to help us navigate and organize sensory information*³²⁰. Because sensory input from the surrounding world has the potential to overload us with too much data and trivial information, mental maps aid us in: creating **heuristics** (or *mental shortcuts*), categorizing objects (such as color), guiding attention, and supporting memory³²¹.

Through **enculturation**, or *the process of learning culture*, people learn the cognitive lens and mental models in which their social groups view, organize, and understand the world³²². This is an important concept to understand while analyzing an organization or individual of a different culture. Growing up in a Western country has ensured that Western norms, values, cognitive models, and mental maps are deeply inscribed into typical Euro-American analyst's "psychological fingerprint". These components are used subconsciously to interact with and understand the world surrounding them, events unfolding in front of them, and other individuals' actions opposing them.

However, the goal of analyzing particular groups or individuals has historically been described as *objectively* understanding that person or groups' past actions, *rationalizing* their current motives, and anticipating their *planned* future behavior. This understanding of the goal of analysis may be fundamentally misleading. As we have read, humans perceive the world, process information, and behave in subjective, biased, and irrational ways that are largely influenced by evolution and enculturation. Assuming that someone will act in an *objective, rational, or planned* way is stripping them of their humanity. The challenges of conducting analysis across

³²⁰ Kenneth J. Guest. *Cultural Anthropology: A Toolkit for a Global Age*. New York, NY: W.W. Norton & Company, 2014. 40.

³²¹ Jennifer S. Blumenthal-Barby, "Biases and heuristics in decision making and their impact on autonomy". *The American Journal of Bioethics* 16, no. 5 (2016): 5–15.

³²² Guest, *Cultural*, 36.

two different cultures (a European-born analyst following and tracking an Afghan farmer turned Taliban operative) are not created because the European-born analyst is allowing culture to “cloud” their judgment, but because the culture that is “clouding” his/her views is vastly different than the culture “clouding” the Taliban operative’s views.

Often, these mental models are strengthened through constant and uniform stimuli. Because of this, humans are likely to develop intuitive and automatic responses to environments with little uncertainty or change. As we will see in the next section, this can either be good or bad, depending on the situation and profession.

Mental Models: Helpful or Harmful?

A useful way to decide whether mental mindsets and models are useful is to look at different professions and their usage within them. Because jobs, sports, and leisurely activities all have unique experiences attributed to them, we can look at each instance as its own culture (or collection of shared experiences). Within these “cultures” we briefly examine some examples where mental models are advantageous, and some where they are not.

In some professions, fixed mental models are directly correlated to performance. People such as poker players, chess masters, and golfers all develop expertise through massive amounts of specific, hyper-focused, and repetitive practice. In these careers, players use “muscle memory” and cognitive equivalents, to intuitively recognize patterns and produce solutions. Chess masters are often quoted as knowing their next move within seconds, only taking more time to explore less plausible alternatives³²³. Through the repetitive study of patterns, players develop an intense domain-specific memory, aimed at recognizing and remembering these patterns once they appear. The amount of repetition required to develop this intuitive sight is so large, psychologists found a competitive chess players’

³²³ David J. Epstein, *Range: Why Generalists Triumph in a Specialized World* (New York City, NY: Riverhead Books, 2019), 25–26.

chance of reaching international master status dropped from one in four to one in fifty-five if they had not begun intense training by age twelve³²⁴. It is important to note, intelligence analysis does not follow suit of the above careers. Specialized expertise developed over decades of repetition do little to aid in an analyst's judgment of a developing and novel situation. These findings suggest that analysts who specialize too narrowly, for too long, may make less accurate judgments and predictions.

As we saw, people who develop domain-specific expertise through repetitive experiences, are often engaged in disciplines with constant statistical regularities, that is, predictable rules govern the patterns with predictable outcomes. People who develop this type of intuitive expertise lose their inherent advantage when rules are slightly altered. A study asked accountants to apply a new tax law to their accounting report – the experienced accountants did worse than the novice ones³²⁵. In another study, scientists gathered experts and nonexperts in the game of bridge to compete. Before the games, however, scientists altered the order of play to the game, surprisingly nonexperts had an easier time adapting to the rule³²⁶. Through the above evidence, we see that developed intuition becomes disadvantageous when the rules and principles surrounding a domain are altered. As somebody reading this might guess, within the analysts' world of geopolitics and global economies, the "rules and principles" rarely remain the same. This shows the importance for analysts to deconstruct and challenge their preconceived notions and mental models of reality. Doing so may allow analysts to begin seeing the world in a whole new way – possibly, more like a scientist.

Impact on Intelligence Community

Intelligence analysis is less like the narrowly focused fields above and more like a science discipline, tasked with exploring the unknown to make sense of the things around us. Much like scientists, analysts cannot intensely and

³²⁴ Epstein, *Range*, 26.

³²⁵ Ibid.

³²⁶ Ibid.

repetitively practice a task in hopes of developing domain-specific mental models. Each situation they encounter has new and unique characteristics. Unfortunately, this does not stop analysts from forming their own mental models and biased perspectives.

Analysts can counter these mental models and fixed mindsets through taking on hobbies and diversifying their education; in other words, by becoming generalists. One study found that scientists with memberships in the highest academies were more likely to have unrelated hobbies outside of work³²⁷. Additionally, Nobel prize winners are twenty-two times more likely to participate in amateur dancing, acting, and other performance types of hobbies³²⁸. Furthermore, compared to other scientists, nationally recognized scientists are more likely to be musicians, sculptors, mechanics, writers, etc. with Nobel prize winners more likely still³²⁹. The creative success of these top engineers and scientists can be partly attributed to their interests outside of their field. Dean Keith Simonton, a psychologist and creativity researcher, states, “rather than obsessively focus[ing] on a narrow topic”, leading scientists have broad interests. He continues, “this breadth often supports insights that cannot be attributed to domain-specific expertise alone.”³³⁰. These studies suggest that intelligence analysts, like scientists, should be encouraged to explore hobbies and interests outside of their focused expertise. These outside interests may help relieve analysts of their fixed perceptions and learned mindsets of the world around them.

Studying past intelligence shortcomings, one will see that analysts’ mindsets are not problematic because they create biases, but rather they are problematic because they create biases that do not align with the biases of the adversary they are studying. Dr. Walton, a senior analyst turned author and professor, notes in his book *Challenges in Intelligence Analysis*, many intelligence shortcomings where analysts were not “thinking like the

³²⁷ Ibid, 32–33.

³²⁸ Ibid.

³²⁹ Epstein, *Range*, 26.

³³⁰ Ibid., 33.

adversary”³³¹. He describes, among many examples, the criticisms outlined in the 9/11 Commission, on the intelligence community not having red teams³³². Red teams are, as defined in the US Department of Defense’s Dictionary of Military and Associated Terms June 2020 edition, “an organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others.”³³³. By not thinking like the enemy, Dr. Walton explains, analysts were not asking the right questions, focusing on the right threats, or collecting the right information. Katherine and Randolph Pherson, back this assertion in their book, *Critical Thinking for Strategic Intelligence*. They write, “almost every postmortem of past intelligence failures concludes that analysts were working from outdated or flawed mental mindsets and had failed to consider alternative explanations.”³³⁴. They continue by commenting on intelligence failures such as the efforts before the 9/11 terrorist attacks “need[ed] to incorporate more rigor and creativity into the analytic process”³³⁵. This evidence suggests that intelligence analysts routinely and historically make faulty assessments because of misaligned cultural mindsets.

Mark Lowenthal – an internationally respected intelligence practitioner, researcher, and author – goes further in his book *Intelligence: From Secrets to Policy*, describing one of the most common flaws in analyst logic – mirror imaging, which he defines as “*assum[ing] that other leaders, states, and groups share motivations or goals similar to those familiar to the analyst.*”³³⁶. Assumptions about the Soviet Union during the Cold War is an example of this. Analysts examined Soviet leaders, attempting

³³¹ Timothy Walton. *Challenges in Intelligence Analysis: Lessons from 1300 BCE to the Present*. New York City, NY: Cambridge University Press, 2010.

³³² “The 9/11 Commission Report”, The 9/11 Commission Report § (2002), <https://govinfo.library.unt.edu/911/report/911Report.pdf>, 339–383.

³³³ “DOD Dictionary of Military and Associated Terms”, www.jcs.mil (Joint Chiefs of Staff, June 2020), <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>, 181.

³³⁴ Pherson, *Critical Thinking*, xxv.

³³⁵ Ibid.

³³⁶ Lowenthal, *Intelligence*, 163.

to categorize them as **hawks** (*a politician favoring military use*) or **doves** (*someone opposing military use*). There was absolutely no evidence to suggest such divisions existed among soviet leaders, but it was assumed the political hierarchy shared similarities with the United States' political system (of which there were plenty hawks and doves). This assumption led analysts down unproductive reasoning paths, resulting in the mischaracterization of Soviet leaders.

As evidence suggests, analysts engaged in methods like red teaming are hindered by their own cultures' mental maps of reality (and mindsets). To counter these culturally learned mindsets, analysts must temporarily but deliberately step away from the western academic institutions that taught us scientific inquiry and causal thinking, Judeo-Christian family structures that taught us values, and nationalistic cultural groups that taught us social norms and cultural mindsets. We have seen how culture directly influences cognition and perception, starting at birth. Only by attempting to strip off western culture can we step outside of western cognition. Only by understanding and attempting to embody our target's culture can we step into the target's mindsets, views, and biases, to understand their cognition. Doing this will help us understand their past biases, examine their current irrationalities, and anticipate their future motives and behavior.

Moving Forward

Analysts face a host of challenges to their analytical thinking. While some challenges arise from our evolutionary past, others are learned through our cultural upbringing. Although SATs and professionalization have attempted to counter these "threats to reason", more work is required on the intelligence communities' part.

Perhaps analysts should receive more encouragement to study alternative disciplines, apart from the traditional cybersecurity, political science, and economics fields. It could be that simply encouraging extracurricular activities and hobbies helps analyst become more generalist. Maybe red teaming operators can use "method-acting" techniques, seen in theatrical studies, to help divest from their cultural mindsets, and adopt their adversary's

cultural mindsets. Or perhaps there are cognitive mechanisms within our brain, evolved to solve an adaptative challenge, that we can use for sound analytical judgments.

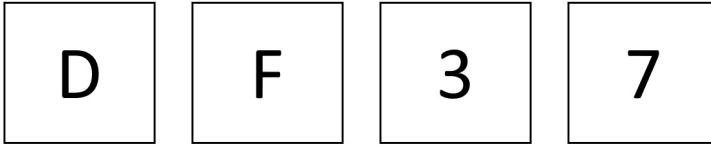
Cheater-Detection

One example of these cognitive mechanisms that may be advantageous is the “cheater-detection” module. Humans possess a tendency to be cooperative with each other³³⁷. However, when you cooperate or do a favor for someone, you temporarily reduce your fitness-level while increasing theirs, but with the expectation that they will do the same when needed. The advantages of exchanging favors and participating in cooperation aid individuals and family units in times of need and strengthen social groups. This tendency towards cooperation (or reciprocal altruism) guides our social behavior and our reasoning ability. Experiments show for a group to adopt a tendency towards reciprocal altruism, it must have the ability to identify and “punish” noncooperators (also called “cheaters” or “defectors”)³³⁸. Engaging in cooperation with a cheater would be costly to that individual; thus, specialized modules within our brain evolved to recognize cheaters.

The following “Wason selection problem” is a simple example of this evolved mechanism that demonstrates the idea that humans are particularly attuned to recognize cheaters. Imagine you are hired as an administrative assistant. Your task is to check a set of documents to confirm they are marked according to the following office rule. “If the document has a D rating, then it must be marked code 3”. Each card below has a letter rating on the front and numerical rating on the back. Which cards must you turn over to check for errors?

³³⁷ Ernst Fehr, and Urs Fischbacher. “The Nature of Human Altruism”. *Nature* 425, no. 6960 (2003): 785–91, <https://doi.org/10.1038/nature02043>.

³³⁸ Michael S. Gazzaniga, Leda Cosmides, and John Tooby. “Social Exchange: The Evolutionary Design of a Neurocognitive System”. In *The Cognitive Neurosciences*, 1295–1308. Cambridge, MA: MIT Press, 2004. <https://psycnet.apa.org/record/2005-01373-087>.



Do you have your answer? Before revealing the correct one, let us look at a second scenario with the same logical structure. Imagine you are hired as a bouncer in a bar. Your task is to check the bar patrons according to the following local law, “If a person is drinking beer, they must be over 20 years old”. Each card below has the person’s age on the front and beverage on the back. Which cards must you turn over to check for lawbreakers?



Do you have your answer? The solution to both questions is the first card and the last card. Chances are, you found the second scenario much easier to solve than the first. In the first scenario, you must ensure the 1st card has a 3 on the back, and the card marked 7 does not have a D on the front – the middle two cards are not restricted to any rules. Likewise, in the second scenario, you must ensure the person drinking the beer is 21, and the 16 year old person is not drinking beer, but there are no restrictions on drinking cola (you can be of any age) or being 25 years old (you are old enough to legally drink alcohol). Both scenarios have the same logical structure, but it is much easier to solve the second scenario.

The hypothesis that explains this difference in solving logically equivalent tasks at different levels of accuracy is that humans are evolved to instinctively detect cheaters within a social situation. If these cheater-detection modules developed in our evolutionary past, they should be apparent in all cultures and ages – and subsequent studies confirm this. The reasoning advantages of cheater-detection strategies have been observed in

children as young as three years old, across many different cultures³³⁹,³⁴⁰. There are two theories in which this cheater-detection module is activated, by combining both, analysts may gain an edge in assessing specific situations.

Social Exchange Theory

Leda Cosmides and John Tooby, two pioneers in evolutionary psychology, issued several Wason selection problems to groups of people and noticed an interesting trend³⁴¹, ³⁴². If the problem contained an element of “cheater-detection” or discerning whether somebody was benefiting from something they were not entitled to (the second scenario) then most participants could solve it. If the problem had no cheaters involved in the logical structure (such as the first scenario), participants had a hard time solving the problem. In their experiment, only 25% of participants solved the first scenario correctly, while 75% were able to solve the second one. Cosmides and Tooby reason reciprocal altruism could not evolve in a widespread and stable manner without the ability to recognize “cheaters” that do not reciprocate cooperation. Their explanation, called **Social Exchange Theory**, proposes these *cheater-detection modules evolved to identify cheaters and preclude them from future social interactions and exchanges*.

This theory was developed further in another study by Gigerenzer and Hug³⁴³. A rule, in the form of a social contract, was described to

³³⁹ Denise Dellarosa Cummins, “Evidence for the innateness of deontic reasoning”. *Mind & Language* 11, no. 2 (1996): 160–190, <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-0017.1996.tb00039.x>.

³⁴⁰ Paul L. Harris, and María Núñez, “Understanding of permission rules by preschool children”, *Child development* 67, no. 4 (1996): 1572–1591, <https://srcd.onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-8624.1996.tb01815.x>.

³⁴¹ Leda Cosmides, “The logic of social exchange: Has natural selection shaped how humans reason? Studies with the Wason selection task”, *Cognition* 31, no. 3 (1989): 187–276. <https://www.sciencedirect.com/science/article/pii/0010027789900231>.

³⁴² Jerome H. Barkow, Leda Cosmides, and John Tooby, eds., *The adapted mind: Evolutionary psychology and the generation of culture*, Oxford University Press, USA, 1992. 163–229.

³⁴³ Gerd Gigerenzer, and Klaus Hug. “Domain-specific reasoning: Social contracts, cheating, and perspective change”. *Cognition* 43, no. 2 (1992): 127–171. <https://www.sciencedirect.com/science/article/pii/001002779290060U>.

participants as follows, “If you stay overnight in a mountain shelter, you must help out by carrying up some firewood to add to the supply.” Both groups of participants were asked to look for violations of the rule; however, group A was asked to look for violations to catch cheaters (cheater-detection), while group B was instructed to look for violations to determine if the rule was in effect (truth/hypothesis-testing). Group A solved the “cheater-detection version” between 78–90% of the time while Group B only solved it correctly around 40% of the time. In conclusion, not only must a social contract be present, but there must also be a possibility of cheating, to activate this module.

Dominance Theory

While the phenomenon of the cheater-detection modules is observed cross-culturally, some anthropologists offer a different theory than Cosmides and Tooby’s one. Dr. Denise Cummins – a renowned cognitive scientist and author – proposes **Dominance Theory**, which states that *cheater-detection is a cognitive adaption to sort through a group of problems surrounding social hierarchies*^{344, 345, 346}. Cheating, in this definition, is simply violating a social norm. Violation detection, Cummins describes, is a function that constrains behavior within one’s social group and maintains status – particularly a dominant position within that social group. Dominant positions are evolutionary beneficial because they have better access to food³⁴⁷, are less likely to be preyed on,³⁴⁸ and have higher

³⁴⁴ Denise Dellarosa Cummins. “Dominance hierarchies and the evolution of human reasoning”. *Minds and Machines* 6, no. 4 (1996): 463–480. <https://link.springer.com/article/10.1007%2FBF00389654>.

³⁴⁵ Denise Dellarosa Cummins. “The evolutionary roots of intelligence and rationality”. *Common Sense, Reasoning, and Rationality*, Oxford UP, Oxford (2002): 132–147.

³⁴⁶ Denise Delarosa Cummins. “Social norms and other minds”. *The evolution of mind* (1998): 30–50. <https://psycnet.apa.org/record/1998-06595-002>.

³⁴⁷ Tim Clutton-Brock and Paul Harvey, Patrick Bateson, Robert Hinde-Brock, T.H., P.H. Harvey, P.P. C. Bateson, and R.A. Hinde. “Growing points in ethology”. (1976): 195–237. https://openlibrary.org/books/OL4880107M/Growing_points_in_ethology.

³⁴⁸ Dorothy L Cheney, and Robert M. Seyfarth. *How monkeys see the world: Inside the mind of another species*. University of Chicago Press, 2018.

reproductive success^{349, 350, 351, 352}. She argues that low-ranking members attempt to improve their social status within a group through cheating and deception^{353, 354, 355}, while dominant individuals maintain hierarchies and priority of access to resources by detecting and stopping attempts to cheat and deceive. Additionally, these dominant social positions are obtained and maintained through alliance formation, largely based on the reciprocal altruism described above^{356, 357, 358, 359}. Therefore, it was a highly adaptive advantage to evolve the cheater-detection modules within all of us.

³⁴⁹ Tim H. Clutton-Brock, ed. *Reproductive success: studies of individual variation in contrasting breeding systems*. University of Chicago Press, 1988.

³⁵⁰ Donald A. Dewsbury. "Dominance rank, copulatory behavior, and differential reproduction". *The Quarterly Review of Biology* 57, no. 2 (1982): 135–159. <https://www.journals.uchicago.edu/doi/abs/10.1086/412672>.

³⁵¹ Lee Ellis. "Dominance and reproductive success among nonhuman animals: a cross-species comparison". *Ethology and sociobiology* 16, no. 4 (1995): 257–333. <https://www.sciencedirect.com/science/article/pii/016230959500050U>.

³⁵² Linda Marie Fedigan. "Dominance and reproductive success in primates". *American Journal of Physical Anthropology* 26, no. S1 (1983): 91–129. <https://onlinelibrary.wiley.com/doi/abs/10.1002/ajpa.1330260506>.

³⁵³ Richard Byrne, and Richard W. Byrne. *The thinking ape: Evolutionary origins of intelligence*. Oxford University Press on Demand, 1995.

³⁵⁴ Robert W. Mitchell, "The psychology of human deception". *Social Research* (1996): 819–861. https://www.jstor.org/stable/40972317?casa_token=X2JzNdkqR7gAAAAA%3A7221pajpJc7CggH2elqRmaul1pPRi6N5mA_NBbVZc71Gm_2Vh7zMfV-R_drXirSzeyl5e9RNHAI9cMU0OuyFPPzesQ4EIMdNAO-JxGShwny_eU6WTug&seq=1#metadata_info_tab_contents.

³⁵⁵ Andrew Whiten and Richard W. Byrne. "The manipulation of attention in primate tactical deception". (1988). <https://psycnet.apa.org/record/1988-98392-016>.

³⁵⁶ Paul L. Vasey, Bernard Chapais, and Carole Gauthier. "Mounting interactions between female Japanese macaques: testing the influence of dominance and aggression". *Ethology* 104, no. 5 (1998): 387–398. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1439-0310.1998.tb00077.x?casa_token=XZoeta3NEHQAAAAA:Rd2QfL86XJlmnca8iHiGnGagzAookH2tSK_Ur_206qwrJI8Vmg_rgExz6lgWmb5el-hWQaEwDK6w_nw.

³⁵⁷ Sudip Datta "Relative power and the acquisition of rank". *Primate social relationships* (1983). <https://ci.nii.ac.jp/naid/10015026754/>.

³⁵⁸ Alexander H. Harcourt. "Alliances in contests and social intelligence". (1988). <https://psycnet.apa.org/record/1988-98392-011>.

³⁵⁹ Robert M., Seyfarth and Dorothy L. Cheney. "Grooming, alliances and reciprocal altruism in vervet monkeys". *Nature* 308, no. 5959 (1984): 541–543. <https://www.nature.com/articles/308541a0>.

This theory was tested by a Wason Selection Experiment, similar to the ones described above³⁶⁰. Student participants were broken into two groups, a cheater-detection group (Group A) and a truth-testing group (Group B). Group A was given an important rule in the dormitory to follow, “if someone is assigned to tutor a study session, that person is required to tape-record the session.”³⁶¹ Similar to other Wason selection tasks, students were told to determine whether the rule was followed with a series of cards. Group B was presented the same rule, but with a different “cue”. They were told to imagine overhearing someone in the hall say, “If I’m assigned to tutor a session, I always tape-record the session”. They were shown the same four cards and told to turn over which ones were needed to know whether or not the person in the hall was telling the truth (truth-testing). Finally, both groups were subdivided into four subgroups: High-ranking, low-ranking, equal high-ranking, and equal low-ranking.

High-ranking: told they were Resident Assistant (RA) checking on students

Low-ranking: told they were a student checking on RAs

Equal high-ranking: told they were an RA checking on other RAs

Equal low-ranking: told they were a student checking on other students

The results validated the Dominance Theory. In every cell, 15–20% of the students correctly identified the violators, except for the “high-ranking” group. The exception, the High-ranking RAs checking the low-ranking students, tripled the percentage correct to 65%. These results mirror the results of the previously reviewed experiment and show how adopting a “high ranking” role within a social group may aid in detecting cheaters (or violators of social rules).

³⁶⁰ Denise Dellarosa Cummins. “Cheater detection is modified by social rank: The impact of dominance on the evolution of cognitive functions”. *Evolution and human behavior* 20, no. 4 (1999): 229–248. https://www.sciencedirect.com/science/article/pii/S1090513899000082?casa_token=WsucrMHDZmcAAAA:tnxFJVcH1A8DFQoiKL-Rb9NI8spqr9nXs8X9c7BmTY3Ncqa80VBvkn3HO4qG7Jf9IhELTyjHMw.

³⁶¹ Ibid.

The Application

An easy example to envision using this “cheater-detection” module as an analyst is to apply it within a social phenomenon accessible and familiar to most humans – competitive sports. In this example, imagine you are a drug investigator for the Tour de France, tasked with investigating potential doping misconduct and performance enhancing drug usage. As an investigator, you want to “get inside the head” of an athlete, to understand their motivations and anticipate their future misconduct. One way of doing this may be to use the innate cognitive mechanisms and learned cultural mindsets discussed throughout this paper (along with SATs).

First, an investigator trying to “activate” their “cheater-detection module might assume the role of a gold medalist cyclist who does not use performance-enhancing drugs or dishonest means to train and compete. By doing this, the investigator assumes a position of dominance within the social hierarchy of cyclists. Doing this evokes the “cheater-detection” module through both the *Social Exchange Theory* and *Dominance Theory*. Furthermore, an investigator trying to “activate” their cultural mindsets with the cyclists may use method-acting techniques used in theater studies to adopt the character of a cyclists. Doing this, the investigator attempts to indoctrinate themselves with the cultural mindsets and mental maps of reality, shared by top-level cyclists. Instead of using structured analytical techniques to objectively and rationally analyze a potential cheating cyclists’ subjective and irrational behavior, they evoke artificially enculturated mindsets and naturally evolved instincts to help ask the right questions, search in the right places, and collect the right information.

Parallel applications for this may be found within: a Security and Exchange Commission’s analysts investigating tax fraud, a DEA agent investigating illegal drug trade, a CIA or FBI analysts investigating election fraud, or a Department of State analyst investigating the misuse of disaster relief funds to a country. As you can see, there is a wide range of applications for domestically engaged or internationally focused analysts.

Conclusion

Innate cognitive mechanisms and learned cultural mindsets have adverse effects on intelligence analysts' objective and logical decision-making. The paper supported this claim by showing (1) intelligence analysts are tasked with possessing objective and logical decision-making skills (2) evolved cognitive mechanisms that cause irrational thinking are innate within all humans (3) learned cultural mindsets adopted from childhood and the environment affect out impartial perception of the world. To counter the adverse effects, agencies have rigorous selection processes, employ structured analytical techniques, and use computer-aided analysis. The later section of the paper explored possible ways in which we might use innate cognitive mechanisms (cheater detection) and artificially learned mindsets (assuming the role of a cyclists) for an additional edge in sound analytical thinking.

Although we continue to develop new technologies and methods that help us collect, assess, and visualize information, humans will forever be at the center of analysis. For as long as the United States continue to exist, sitting at the CIA's desk in its Langley headquarters, will be an analyst defined by their evolutionary past and cultural upbringing – the American Ape.

Yea or Nay on Huawei? Altering the Balance of the 5G Technology War in Europe

Jefferson T. STAMP

Abstract: Although the potential security threat posed by Huawei's 5G technology has been under review for more than a year, Europe still lacks a unified response. The indecision is due in part to NATO's inability to address technology-based security issues that arise from international trade. To combat European ambivalence, the U.S. strategy has been to render Huawei an unreliable vendor in 5G development through the enforcement of export controls. In effect, the U.S. is using its hegemonic power in the international trading system to coerce European countries into an emerging technology-based security regime in opposition to the Chinese surveillance state. The research presented herein explores Huawei's technological disruption in the geopolitical context of strategic information warfare and examines how these factors color the current debate. The research demonstrates that, when making their ultimate decision on Huawei's 5G technology, European countries should consider the impact of technological disruption and strategic information warfare on the integrity of the international system as well as the importance of retaining sovereignty over critical infrastructure in the maintenance of their democratic societies and values.

Keywords: telecommunications, Huawei, 5G, technological disruption, strategic information warfare, surveillance, security, intelligence, NATO, export controls, hegemony, geopolitical

Introduction

European countries have been reviewing the security threat posed by Huawei's 5G technology for more than a year³⁶². Of course, a quick 5G rollout using Huawei's telecommunications equipment could provide dramatic economic benefits. In the Information Age, efficient communication of large amounts of data is the key to generating wealth from data-driven goods and services³⁶³. Representing the next generation in data transmission capability³⁶⁴, "5G could be the start of another round of innovation and growth similar to what we saw with the arrival of the internet...."³⁶⁵. As the current leader and cheapest supplier of 5G technology³⁶⁶, Huawei is well-positioned to develop 5G infrastructure throughout the world³⁶⁷. On the other hand, if Huawei is restricted from 5G development, "European politicians fear falling further behind...."³⁶⁸. They also fear retaliation from China banning European products from the lucrative Chinese market³⁶⁹. Thus, the pragmatic approach has been to manage the potential security risks associated with utilizing Huawei's 5G technology without sacrificing the economic benefits.

³⁶² Saqib Shah, Liz Thomas and Cat Weeks, "Europe lacks a unified approach to Huawei despite yearlong assessments", *S&P Global Market Intelligence*, July 27, 2020, <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/europe-lacks-unified-approach-to-huawei-despite-yearlong-assessments-59602291>, (accessed August 8, 2020).

³⁶³ James Lewis, "Can Telephones Race? 5G and the Evolution of Telecom Part I", *Center for Strategic International Studies*, (2020): 3.

³⁶⁴ "Mobile wireless technology has evolved over four generations: voice calls in the 1980s (1G), messaging in the 1990s (2G), limited multimedia, text and internet data in the late 1990s and early 2000s (3G), and true data with dynamic information access and variable devices in the late 2000s (4G and LTE)". Andrea Gilli, "NATO & 5G: what strategic lessons?", *NATO Defense College*, no. 13 (July 2020): 1, <https://www.jstor.org/stable/resrep25095>, (accessed August 6, 2020).

³⁶⁵ *Ibid.*

³⁶⁶ Lindsay Maizland and Andrew Chatzky, "Huawei: China's Controversial Tech Giant", *Council on Foreign Relations*, August 6, 2020, <https://www.cfr.org/background/huawei-chinas-controversial-tech-giant> (1/12, 8/12), (accessed August 23, 2020).

³⁶⁷ "Huawei and 5G – The European Theatre", *The Economist*, July 18, 2020, 16.

³⁶⁸ *Ibid.*

³⁶⁹ *Id.*, 17 ("Chinese reprisals against countries chucking out Huawei can be expected...").

From a security analyst perspective however, it is Europe's ambivalence which itself presents the strategic lesson³⁷⁰. As pointed out by Andrea Gilli of the NATO Defense College, "this is the first time since the end of World War II that a leader of a key technology is neither an Ally nor a NATO/western country."³⁷¹ Europe's lack of unity on Huawei reflects two competing technology paradigms; one that is focused on technology-based economic development grounded in globalism and free trade, while the other is focused on an emerging bipolar and technology-based security regime. The tension between these two paradigms highlights a shortcoming in NATO's limited construction as a "military alliance of democracies which was not designed to deal with trade policy, industrial leadership and market competition in the world of high-tech."³⁷² The result has been the lack of a unified position after more than year of assessing the security threat.

Given the lack of a unified response by European countries, the containment of Huawei is now being driven by the United States as the hegemonic power in the international trading system. Specifically, the U.S. has imposed export controls which siphon Huawei's supply chain of critical U.S. technology such as semiconductors³⁷³. "Without U.S. technology, Huawei will be hard-pressed to make 5G infrastructure products..."³⁷⁴.

The U.S. trade restrictions will no doubt force the Chinese government to develop its own internal supply chains. In this respect, "[e]xport controls on chips and chip-manufacturing might well have diminishing returns. A lack of competition from Western technology could simply help China build its industry in the long run."³⁷⁵ The U.S. export controls may also be

³⁷⁰ Gilli, "NATO & 5G: what strategic lessons?", 4.

³⁷¹ Ibid., 3.

³⁷² Ibid., 4.

³⁷³ Michael R. Pompeo, U.S. Secretary of State, "The United States Protects National Security and the Integrity of 5G Networks", U.S. Department of State, May 15, 2020, <https://www.state.gov/the-united-states-protects-the-national-security-and-the-integrity-of-5g-networks> (1/4), (accessed July 25, 2020).

³⁷⁴ James Lewis, "Can Telephones Race? 5G and the Evolution of Telecom Part I", 4.

³⁷⁵ Ben Buchanan, "The U.S. has AI Competition All Wrong", *Foreign Affairs*, August 7, 2020, <https://www.foreignaffairs.com/articles/united-states/2020-08-07/us-has-ai-competition-all-wrong> (5/9).

undermined from alternative sources in competing nations³⁷⁶. For these reasons, Bown argues that successful export controls against Huawei should be “multilateralized” so that other countries cooperate in restricting substitute supplies to Huawei³⁷⁷. “However, the supply chain for telecom will depend on semiconductors and specialized software, all areas where the United States has a substantial lead.”³⁷⁸. Thus, the unilateral approach by the U.S. may be still successful in at least temporarily stifling Huawei’s drive to develop the world’s 5G infrastructure because the export controls are focused on a supply chain that the U.S. currently dominates.

The immediate aim of this U.S. policy is seemingly to coerce Europe into an alignment of democratic countries within an emerging bipolar techno-security regime. If that is the case, the decision over Huawei’s 5G technology is one to be made in the current geopolitical context; *i.e.*, will European nations utilize and rely upon the lesser developed technology from a democratic source committed to the relatively free flow of data and thereby maintain sovereignty over their telecommunications network, or will they utilize and rely upon the expedient technology from a communist source that is undergirding the Chinese surveillance state and projecting the power of the Chinese Communist Party?

In order to determine how best to answer the question about Huawei, the following research focuses on a brief history of technological disruption and strategic information warfare, the resulting 5G security threat in light of Huawei’s role within China’s surveillance state and the effect of U.S. export controls on the balance of the 5G technology war.

³⁷⁶ Chad P. Bown, “Export Controls: America’s Other National Security Threat”, *Duke Journal of Comparative & International Law*, 30 (2020): 291–292, <https://www.scholarship.law.duke.edu/djcil/vol30/iss2/4>, (accessed August 1, 2020).

³⁷⁷ *Ibid.*, 291.

³⁷⁸ Lewis, 8.

Brief History of Technological Disruption and Strategic Information Warfare

One of the greatest lessons in human history is the importance of technology in military affairs and how technological revolutions can redefine the world order. At the beginning of this century, Max Boot explained how advances in technology affect the international system: “Over the last 500 years, the fate of nations has been increasingly tied to their success, or lack thereof, in harnessing revolutions in military affairs. These are periods of momentous change when new technologies combine with new doctrines and new forms of organization to transform not only the face of battle but also the nature of the state and the international system.”³⁷⁹.

The Mongols, as Boots highlights, maintained the “mightiest military forces” until the 15th century when they failed to “keep pace with the spread of gunpowder weapons and the rise of centralized governments that used them.”³⁸⁰. Implicit in the centralization of government control was the ability to harness national communications such as the semaphore system of telegraphs in Revolutionary and Napoleonic France³⁸¹. Schofield asserts, “From the outset, the prime purpose [of this communications network] was military.”³⁸². However, Dumas famously depicted how such a network could be compromised to spread disinformation and cause a financial panic in *The Count of Monte Cristo*³⁸³.

³⁷⁹ Max Boot, “Are we the Mongols of the Information Age?”, *Los Angeles Times*, October 29, 2006, <https://www.latimes.com/archives/la-xpm-2006-oct-29-op-boot29-story.html> (1/5), (accessed August 4, 2020).

³⁸⁰ Ibid.

³⁸¹ Patrice Flichy, “The Birth of Long Distance Communication. Semaphore Telegraphs in Europe”, *Réseaux. The French Journal of Communication*, 1.1 (1993): 81–101, https://www.persee.fr/doc/reso_0969-9864_1993_num_1_1_3272, (accessed August 9, 2020).

³⁸² Hugh Schofield, “How Napoleon’s semaphore telegraph changed the world”, *BBC News Magazine*, June 17, 2013, <https://www.bbc.com/news/magazine-22909590> (4/16), (accessed August 15, 2020).

³⁸³ David Alan Grier, “What the Count of Monte Cristo Can Teach Us About Cybersecurity”, *IEEE Spectrum*, January 25, 2018, <https://spectrum.ieee.org/tech-talk/telecom/security/what-the-count-of-monte-cristo-can-teach-us-about-cybersecurity>, (accessed August 17, 2020).

“Historically”, Gilli argues, “communications have been at the centre of geopolitical competition among countries.”³⁸⁴ By the 20th century, one of the first examples of “strategic information warfare” was the British plan “to cut German undersea cables across the world.”³⁸⁵ Taking advantage of its control over a global network of colonial outposts, “Britain’s strategy was to deprive Germany of its outside communications and force communications from German cables onto British-controlled wires, where they could be collected and decrypted.”³⁸⁶ As a result, Britain was able to “use cable cutting and censorship as strategic resources in World War I.”³⁸⁷

Subsequently, “Radio itself altered the conceptualization of international communications. Radio enabled governments to control their own infrastructure.”³⁸⁸ This new technology neutralized British hegemony over communications, and combined with electronics, helped set the stage for the “Information Revolution” after World War II. Computer technology, in turn, ushered in a new world order. Boot points out, “The Soviet Union had no Silicon Valley and could not compete with the United States in incorporating the computer into its economic or military spheres. U.S. prowess at waging war in the Information Age was showcased in the 1991 Persian Gulf War, which, along with the collapse of the Soviet empire, left the United States standing alone as a global hegemon.”³⁸⁹

³⁸⁴ Gilli, “Nato and 5G: what strategic lessons?”, 2.

³⁸⁵ Calder Walton, “China Will Use Huawei to Spy Because So Would You”, *Foreign Policy*, July 14, 2020, <https://foreignpolicy.com/2020/07/14/britain-boris-johnson-china-will-use-huawei-to-spy-because-so-would-you> (3/14), (accessed July 15, 2020).

³⁸⁶ Ibid.

³⁸⁷ Jill Hills, *The Struggle for Control of Global Communication*, (University of Illinois Press, 2002), 286, <https://www.jstor.org/stable/10.5406/j.ctt2ttcks.13>, (accessed August 6, 2020).

³⁸⁸ Ibid., 288.

³⁸⁹ Boot, (2/5).

The 5G Security Threat posed by China's Huawei in Strategic Information Warfare

With the advent of the computer and the Internet, the age of wireless telecommunications presents a new set of opportunities for strategic information warfare. At the same time, history's lessons for nations to maintain control of their information technology infrastructure, provides a guide for insulating against these modern security threats.

A recent study by Ainikki Riikonen argues, "Information architecture—the structures of technology that collect and relay information worldwide—is innately connected to power projection."³⁹⁰ Starting from this thesis, Riikonen warns that China has been the most innovative in this area and is doing so in a manner that threatens the very foundation of democratic governance. Specifically, "the PRC will weaponize connectivity and employ technologies that maximize the CCP's agency over the availability and flow of information. Agency over information architecture is a potent tool for states in understanding and shaping the international environment and in winning both political and military confrontations."³⁹¹

When assessing agency over information architecture, there are at least three spheres of vulnerability that result from the use of Huawei's 5G equipment in a telecommunications system. First, "tech-enabled connectivity" is what is viewed by China as "the back bone of U.S. military superiority" because technology now provides the infrastructure for all U.S. military operations, including command and control³⁹². By focusing on gaining an edge in information technology infrastructure, China could potentially undermine U.S. operations by cutting the cyberspace "cables" upon which all U.S. communications depend.

For at least the past decade, the U.S. has formally recognized the threat to "commercial information technology, or IT, infrastructure" as a "new

³⁹⁰ Ainikki Riikonen, "Decide, Disrupt, Destroy", *Strategic Studies Quarterly*, 13, no. 4, (Winter 2019): 122, <https://www.jstor.org/stable/10.2307/26815049>, (accessed July 25, 2020).

³⁹¹ *Ibid.*, 123.

³⁹² *Ibid.*

asymmetry in future warfare.”³⁹³. Digital war games conducted by Australia in early 2018 have similarly exposed China’s “offensive potential” from having “access to equipment installed in the 5G network.”³⁹⁴. As Sanger and Brooks discuss, “the struggle over 5G is about far more than trade or technical advantage. It is about the power to control a nation’s infrastructure—and, in time of conflict, to cut off an adversary’s ability to communicate. And that makes the geopolitics as important as the technology.”³⁹⁵.

Given this vulnerability, it is highly unlikely that U.S. forces would undertake significant operations in defense of any NATO country with a Huawei-based telecommunications infrastructure. To do so would effectively cede China the power to cut off all communications in a time of conflict or crisis. Consequently, European countries “could inject serious risk” to “defense cooperation” with the United States if they allow Huawei to build their 5G telecommunications network³⁹⁶.

The second sphere of vulnerability concerns espionage. Walton explains that “Huawei’s presence on [a] 5G network could allow Beijing to conduct economic espionage ... [and] also collect ostensibly nonsensitive bulk data....”³⁹⁷. This bulk data may inadvertently reveal more sensitive information from “defense, security and intelligence services.”³⁹⁸. Given this vulnerability, the U.S. has threatened to withhold intelligence from any NATO country that uses Huawei technology in its telecommunications infrastruc-

³⁹³ Cheryl Pellerin, “Lynn: cyberspace is new domain of warfare”, Armed Forces Press Service, CENTCOM (October 19, 2010), <https://centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/884164/lyn-cyberspace-is-new-domain-of-warfare> (1/4), (accessed August 15, 2020).

³⁹⁴ Casell Bryan-Low, Colin Packham, David Lague, Steve Stecklow and Jack Stubbs, “Hobbling Huawei: Inside the U.S. war on China’s tech giant”, *Reuters*, May 21, 2019, <https://www.reuters.com/investigates/special-report/huawei-usa-campaign> (3/15), (accessed July 25, 2020).

³⁹⁵ David A. Sanger and Mary K. Brooks, “Battlefield 5G: Are the U.S. and China destined for a forever-war over network control?”, *Wilson Quarterly* (Spring 2020), <https://www.wilsonquarterly.com/who-writes-the-rules/battlefield-5g> (2/11), (accessed August 22, 2020).

³⁹⁶ Mark T. Esper, U.S. Secretary of Defense, “As Prepared Remarks by Secretary of Defense Mark T. Esper at the Munich Security Conference”, U.S. Department of Defense, February 15, 2020, <https://defense.gov/Newsroom/Speeches/Speech/Article/2085577/as-prepared-remarks-by-secretary-of-defense-mark-t-esper-at-the-munich-security> (6/8), (accessed August 15, 2020).

³⁹⁷ Walton, “China Will Use Huawei to Spy Because So Would You”, (13/14).

³⁹⁸ *Ibid.*

ture. As explained by U.S. Defense Secretary Esper: “Reliance on Chinese 5G vendors ... could render our partners’ critical systems vulnerable to disruption, manipulation and espionage. It could also jeopardize our communication and intelligence sharing capabilities, and by extension, our alliances.”³⁹⁹.

In addition, the 5G data stream controlled by Huawei could provide China information from virtually all devices connected via the Internet of Things, disclosing industrial processes and an infinite array of data points that will improve China’s Artificial Intelligence and other technical applications. “The true scale of the threat posed by 5G Huawei hardware becomes clear when we consider how it could be combined with billions of internet-enabled devices, sensors, and gadgets in households, offices, and infrastructure, most of which are unsecured and whose owners may not even know are networked. They would effectively constitute billions of backdoors....”⁴⁰⁰.

Utilizing this massive database, “Chinese scientists could use a rapidly developing methodology called ‘social network analysis,’ which reveals nonobvious relationships between places and people, for intelligence targeting....”⁴⁰¹. The potentially limitless cache of data and new applications from Huawei’s 5G networks would provide China a several degrees of magnitude advantage both in military and industrial decision-making, and also present China with a perfect platform for spreading disinformation.

The third sphere of vulnerability is in the area of cyberattacks. In November 2019, the European Union Agency for Cybersecurity (ENISA) issued its report on the “Threat Landscape for 5G Networks”, detailing ENISA’s “threat assessment for the 5th generation of mobile telecommunications networks.” Among the comprehensive list of enumerated threats, one threat stands out – the threat from “nation states” and the relationship they may have to 5G vendors.

³⁹⁹ Esper, “Munich Security Conference”, (7/8).

⁴⁰⁰ Walton, (13/14).

⁴⁰¹ Ibid.

The ENISA report concludes: “It is indisputable that vendors of 5G components – just like any other technology vendor – are in a better position to cause devastating attacks to the operation of self-developed components, especially when governments influence them. Given the importance of 5G to the sovereignty of nation-states, they will probably be a target of state-sponsored attacks.”⁴⁰². While no vendor was singled out, the report unmistakably describes the cyber-security threat posed by the largest 5G vendors in the world, including China's Huawei. Only upon review of Huawei's role in China's surveillance state can the threat be fully appreciated.

Huawei's role in the Surveillance State and China's policy of Military-Civil Fusion

At the heart of the emerging Chinese surveillance state is the collection of data by technology companies like Huawei. In an article by the Epoch Times in 2018, it was reported that Huawei “plays a pivotal role in establishing high-tech totalitarianism across China's cities [and] provinces.”⁴⁰³. Specifically, Huawei has assisted in the Chinese Communist Party's creation of an “urban digitization scheme” called “China Skynet” in order to “surveil 1.4 billion Chinese people, suppress political opponents, and persecute minorities.”⁴⁰⁴.

It was further reported that the Chinese surveillance system includes more than 170 million cameras with more than 400 million cameras planned for installation over a period of three years⁴⁰⁵. For its part, Huawei led the development of the facial recognition software that is used by the govern-

⁴⁰² Marco Laurencio and Louis Marinos, “ENISA Threat Landscape for 5G Networks”, *European Union Agency for Cybersecurity*, (November 2019): 72, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>, (accessed August 1, 2020).

⁴⁰³ He Jian, “Huawei and the Creation of China's Orwellian Surveillance State”, *The Epoch Times*, December 24, 2018, updated January 8, 2019, https://www.theepochtimes.com/huawei-and-the-creation-of-chinas-orwellian-surveillance-state_2747922.html (1/8), (accessed July 25, 2020).

⁴⁰⁴ *Ibid.*, (2/8).

⁴⁰⁵ *Ibid.*

ment to keep track of every individual citizen⁴⁰⁶. Huawei technology has also been used in the massive surveillance and detention of the Uyghurs in the Xinjiang province⁴⁰⁷. Based on omnipresent technological surveillance and the perpetual accumulation of personal data, a “citizen score” rates the entire population on their obedience to the state⁴⁰⁸.

The participation of Huawei and other technology companies in massive state surveillance raises questions about the role of such companies in society⁴⁰⁹. Are these profit-making ventures merely assisting the government in the mass surveillance of the general population for some public good such as the reduction of terrorism? Or are these companies actually extensions of the Chinese Communist Party embracing an integral role in the maintenance of power and oppression over the general population? The history of Huawei strongly suggests the latter is the case.

From its founding in the 1980’s, Huawei “has had ties with the People’s Liberation Army (PLA) and other security apparatuses of the Chinese party-state.”⁴¹⁰. Umback’s study confirms that: “Huawei has received strong political support from the Chinese party-state since its infancy, and that support proved instrumental in its initial survival and subsequent global expansion. Today, it occupies a key position in major initiatives of the party-state, including the ‘Digital Silk Road’ component of the Belt and Road Initiative and the strategy of ‘civil-military fusion.’”⁴¹¹.

In 2016, Chinese President Xi Jinping adopted “civil-military fusion” as a formal policy to enhance “the development of dual-use technology and [to] integrate existing civilian technologies into the arsenal of the People’s

⁴⁰⁶ Ibid.

⁴⁰⁷ Ibid., (4–5/8).

⁴⁰⁸ Anna Mitchell and Larry Diamond, “China’s Surveillance State Should Scare Everyone”, *The Atlantic*, February 2, 2018, <https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/> (2/6), (accessed July 18, 2020).

⁴⁰⁹ Ibid., (3/6).

⁴¹⁰ Rick Umback, “Huawei and Telefunken: Communications enterprises and rising power strategies”, *Strategic Insights*, (Australian Strategic Policy Institute, 2019): 7, <http://www.jstor.com/stable/resrep23012>, (accessed August 6, 2020).

⁴¹¹ Ibid., 6.

Liberation Army.”⁴¹². Moreover, China's National Intelligence Law, adopted the following year, requires all business organizations to “support, cooperate with and collaborate in national intelligence work.”⁴¹³. Pursuant to this legal authority, Chinese companies simply do not “have the option of turning down government requests to share technology.”⁴¹⁴. Yi-Zheng Lian points out, “Spying for the state is a duty of the citizens and corporations of China under the law, much like paying taxes.”⁴¹⁵. Considering Huawei's history and the policy of civil-military fusion, Huawei is inescapably intertwined within the Chinese military-industrial-complex. Accordingly, the U.S. Defense Department has identified Huawei as being owned or controlled by China's military⁴¹⁶.

Faced with the reality of Huawei's connections to the Chinese surveillance state, European countries must consider the security implications of relying on Huawei's 5G technology in the context of geopolitics and strategic information warfare. First, opting for Huawei is tantamount to placing control of the state's 5G networks in the hands of the Chinese government. Under this scenario, the telecommunications and data flows supporting the entirety of society could be surveilled, manipulated and undermined by China for political and military purposes. Reliance on Huawei in this manner is, therefore, fundamentally at odds with European democratic values and ultimately jeopardizes the very sovereignty of targeted democratic states. Accordingly, an analysis of the hybrid aspects of high technology must constitute part of the calculus of any nation state when assessing the security threat from Huawei. Democratic governments in particular,

⁴¹² Anja Manuel and Kathleen Hicks, “Can China's Military win the Tech War? How the United States Should-and Should Not-Counter Beijing's Civil-Military Fusion”, *Foreign Affairs*, July 29, 2020, <https://www.foreignaffairs.com/articles/united-states/2020-07-29/can-chinas-military-win-tech-war> (2/12), (accessed July 29, 2020).

⁴¹³ Maizland and Chatzky, “Huawei: China's Controversial Tech Giant”, (6/12).

⁴¹⁴ *Ibid.*, (3/12).

⁴¹⁵ Yi-Zheng Lian, “Where Spying is the Law”, *The New York Times*, March 13, 2019, <https://www.nytimes.com/2019/03/13/opinion/china-canada-huawei-spying-espionage-5g.html> (1/2), (accessed August 23, 2020).

⁴¹⁶ Tony Capaccio and Jenny Leonard, “Huawei on List of 20 Chinese Companies that Pentagon Says Are Controlled by People's Liberation Army”, *Time*, June 25, 2020, <https://time.com/5859119/huawei-chinese-military-company-list>, (accessed July 25, 2020).

given their relative freedom and openness, are the most vulnerable to the types of subversion and sabotage of telecommunications networks that would be possible under the Orwellian world interposed by China through Huawei's 5G technology.

The Use of U.S. Export Controls to Alter the Balance of the 5G Technology War

Notwithstanding the security concerns outlined above, democratic countries in Europe have been reluctant in making the switch from Huawei⁴¹⁷. "While telecoms operators in the bloc have called for clarity on government policies towards Huawei", Shah, Thomas and Weeks argue, "the region is still highly divided, with almost an equal number of countries excluding and including the Chinese company from 5G rollouts."⁴¹⁸

One reason for the division in Europe is that the United States itself does not have an exemplary record for respecting the sanctity of international telecommunications security. Thus, "at its most basic level, the U.S. versus Huawei fight is also a raw geopolitical competition between two superpowers with advanced signals intelligence capabilities and extremely pervasive global surveillance networks."⁴¹⁹ The U.S. response seems to be that western intelligence agencies, unlike China's security apparatus, are " beholden to democratic legal systems and respect for human rights and political speech."⁴²⁰ While not exactly reassuring to the skeptics and cynics, there is no denying an element of *realpolitik* as a critical factor in the debate. In effect, the U.S. is leveraging its position in the current world order as the ultimate safe refuge for democratic institutions and the people who yearn for them.

⁴¹⁷ Shah, Thomas and Weeks, "Europe lacks unified approach to Huawei despite yearlong assessments", (1/4).

⁴¹⁸ Ibid., (2/4).

⁴¹⁹ Garret M. Graff, "Could Trump Win the War on Huawei—and Is Tik Tok Next?", July 14, 2020, <https://www.wired.com/story/could-trump-win-the-war-on-huawei-and-is-tiktok-next> (10/15), (accessed July 25, 2020).

⁴²⁰ Ibid.

When viewed in this light, it is not surprising that the U.S. was able to gain its initial foothold for restrictive commitments against Huawei in a group of three Eastern European countries—Romania, Poland and Estonia⁴²¹. As such, Brinza found that the U.S. security guarantee paved the way for a 5G solution among these allies that will be completely Huawei-free: “While China may hold leverage in the form of some unfulfilled investments, the United States is the security guarantee that can keep Central and Eastern Europe free from the perceived Russian threat. That is why the United States succeeded in signing its first anti-Huawei memorandum of understanding in Eastern, not Western, Europe.”⁴²².

Western European countries, including the E.U. as a whole, have been more deliberative. In March 2019, the European Commission issued a voluntary recommendation for each European state to generically assess the cybersecurity risks of 5G networks, including “the overall risk of influence by a third country...”⁴²³. While talks were anticipated to continue throughout the year, it was clear from the Commission’s recommendation that “Washington failed to get its Huawei ban....”⁴²⁴. Instead, the plan was to review the issues and “demand stricter security measures on telecoms vendors by the end of the year.”⁴²⁵.

The year lapsed with Prime Minister Boris Johnson’s decision in January 2020 which “approved a substantial if clearly demarcated role for Huawei in Britain’s 5G telecoms infrastructure.”⁴²⁶. The decision was justified on the grounds that established procedures would safeguard Britain’s “core” infrastructure, and also that Huawei’s equipment could be relegated to the

⁴²¹ Andreea Brinza, “How Russia helped the United States fight Huawei in Central and Eastern Europe”, *War on the Rocks*, March 12, 2020, <https://www.warontherocks.com/2020/03/how-russia-helped-the-united-states-fight-huawei-in-central-and-eastern-europe> (2/8), (accessed July 25, 2020).

⁴²² *Ibid.*, (7/8).

⁴²³ European Commission, “Commission Recommendation – Cybersecurity of 5G networks”, March 26, 2019, 4, <https://www.ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks>, (accessed August 1, 2020).

⁴²⁴ Laurens Cerulus, “7 takeaways on the EU’s Huawei plan”, *Politico*, March 26, 2019, <https://www.politico.eu/article/europe-huawei-7-takeaways-on-plan> (3–4/6), (accessed August 8, 2020).

⁴²⁵ *Ibid.*, (2/6).

⁴²⁶ “Huawei and 5G – The European Theatre”, *The Economist*, July 18, 2020, 15.

“non-core” components of the network⁴²⁷. In this manner, “Britain could get its 5G systems up and running considerably sooner, and cheaper, than would otherwise be possible.”⁴²⁸.

Having been rejected by its closest of allies, the U.S. was forced to employ its hegemonic power in the international trading system to coerce its democratic brethren into excluding Huawei. On May 15, 2020, the U.S. announced it was adopting a set of stringent export controls barring the sale or transfer of any U.S. technology to Huawei⁴²⁹. This new restriction is intended to apply globally. As explained by U.S. Secretary of State Pompeo: “It also imposes U.S. export controls on countries that use U.S. technology or software to design and produce semiconductors for Huawei. Companies wishing to sell certain items to Huawei must now obtain a license from the United States government.”⁴³⁰.

With its supply chain now under siege, Huawei has quickly become an unreliable vendor. As reported by NPR: “Analysts say this latest move likely spells a death knell for Huawei’s global ambitions by freezing out the Chinese company from fundamental semiconductor technology and by raising the costs for hundreds of countries that were relying on Huawei components for their 5G expansion plans, including many in Europe.”⁴³¹. According to Alex Capri at the National University of Singapore, this is a “watershed moment because it’s the beginning of an emerging technological reality.”⁴³². A former British diplomat acknowledged the geopolitical reality: “There was a bit of a checkmate by the U.S.”⁴³³.

⁴²⁷ Ibid.

⁴²⁸ Ibid.

⁴²⁹ Michael R. Pompeo, U.S. Secretary of State, “The United States Protects National Security and Integrity of 5G Networks”, U.S. Department of State, May 15, 2020, <https://www.state.gov/the-united-states-protects-national-security-and-the-integrity-of-5g-networks> (1/4), (accessed July 25, 2020).

⁴³⁰ Ibid.

⁴³¹ Emily Feng, “The Latest U.S. Blow to China’s Huawei Could Knock Out Its Global 5G Plans”, *NPR*, May 28, 2020, <https://www.npr.org/2020/05/28/862658646/the-latest-u-s-blow-to-chinas-huawei-could-knock-out-its-global-5g-plans> (2/10), (accessed July 27, 2020).

⁴³² Ibid., (3/10).

⁴³³ Adam Satariano, Stephen Castle and David E. Sanger, “U.K. Bars Huawei for 5G as Tech Battle Between China and the West Escalates”, *The New York Times*, July 14, 2020, <https://www.nytimes.com/2020/07/14/business/huawei-uk-5g.html> (2/3), (accessed August 17, 2020).

The U.S. “decoupling” from the China matrix will inevitably force every democratic country in Europe to make a “binary choice” between the two technological paradigms, resulting in a “bifurcation of the global economy.”⁴³⁴ On July 14, 2020, two months after the U.S. imposition of global export controls on Huawei, the British government reversed its earlier decision and announced that it was banning Huawei equipment from its 5G networks⁴³⁵. Moreover, any currently installed Huawei equipment must be removed by 2027⁴³⁶. The reversal is estimated to delay Britain’s implementation of 5G approximately two to three years with an estimated cost of about 2 billion pounds⁴³⁷.

At the same time, Prime Minister Johnson is now proposing a “new institution” consisting of “an alliance of ten leading democracies—consisting of the G-7 countries plus Australia, India and South Korea and dubbed the ‘D10’—to coordinate telecom policy and develop an alternative to China’s market leader Huawei....”⁴³⁸. Thus, in an ironic twist, the new push for multilateralism in the fight against Huawei, which was originally viewed by some as a condition precedent for any successful enforcement of U.S. export controls, has actually been triggered by the unilateral action by the U.S.

While the story of this new multilateralism is still unfolding, it is fair to say that the U.S. export controls are beginning to alter the balance in the 5G technology war in Europe. As stated by U.S. Secretary of State Pompeo, “The tide is turning against Huawei as citizens around the world are waking up to the danger of the Chinese Communist Party’s surveillance state.”⁴³⁹.

⁴³⁴ Darren J. Lim and Victor Ferguson, “Conscious Decoupling: The Technology Security Dilemma”, in *China Dreams*, Eds. Jane Golley, Linda Javin, Ben Hillman, Sharon Strange (ANU Press, 2020), 120.

⁴³⁵ Satariano, Castle and Sanger, (1/3).

⁴³⁶ “Huawei and 5G – The European Theatre”, *The Economist*, July 18, 2020, 15.

⁴³⁷ *Ibid.*, 16.

⁴³⁸ Edward Fishman and Siddharth Mohandas, “A Council of Democracies Can Save Multilateralism”, *Foreign Affairs*, August 3, 2020, <https://foreignaffairs.com/articles/asia/2020-08-03/council-democracies-can-save-multilateralism> (2/10), (accessed August 3, 2020).

⁴³⁹ Michael R. Pompeo, U.S. Secretary of State, “The Tide is Turning Toward Trusted 5G Vendors”, June 24, 2020, <https://www.state.gov/the-tide-is-turning-toward-trusted-5g-vendors> (1/4) (accessed July 25, 2020).

Conclusion

The security challenge posed by Huawei in the development of 5G telecommunications networks concerns the potential vulnerabilities of democratic nations to high-tech surveillance and the loss of sovereignty over critical infrastructure. Because of Huawei's connections to the Chinese government, virtually all wireless communications and data transfers could be subject to the control of the Chinese surveillance state.

In response to European ambivalence on this issue, the U.S. strategy has been to render Huawei an unreliable vendor in 5G development through the enforcement of export controls. In effect, the U.S. is using its hegemonic power in the international trading system to coerce European countries into an emerging technology-based security regime in opposition to the Chinese surveillance state.

The research presented herein has explored Huawei's technological disruption in the geopolitical context of strategic information warfare and examined how these factors color the current debate. The research demonstrates that, when making their ultimate decision on Huawei, European countries should consider the impact of technological disruption and strategic information warfare on the integrity of the international system as well as the importance of retaining sovereignty over critical infrastructure in the maintenance of their democratic societies and values. When these considerations are taken into account, it seems clear that European countries should develop an alternative 5G telecommunications network, de-link from the Chinese technology matrix and align with the U.S. in a new technology-based security regime.

Threat Assessment of Chemical and Biological Warfare

Lauren EDSON

Executive summary: The weaponization of chemicals and biological agents have higher mortality rates and demoralizing effects than conventional weapons, and thus considered weapons of mass destruction (WMD). Since World War I, the use of chemical warfare has dominated the international stage. Multiple countries have conducted extensive biological R&D and acquired an advanced capability, however aside from toxins, there has been less actual deployment of biological weapons. Nevertheless, recent advances in biotechnology allow for more advanced weaponization of biological agents. After the proliferation and use of these unconventional weapons globally, the international community started to acknowledge the inhumane and demoralizing effects of them and as a result, security apparatuses to prevent proliferation and prohibit the use of them through international agreements, conventions and organizations. History shows that countries have violated international agreements. Countries with an extensive chemical and biological infrastructure, are considered potential actors to weaponize these materials, as many equipment, supplies, and facilities care considered dual-use in which they can be used for both peaceful and military purposes. Additionally, major difficulties arise in the verifying the use of these weapons and attributing blame as confirmation of allegations often takes time. Nevertheless, it is important to monitor countries who are likely to have capability and intentions to use these weapons such as Russia, Syria, North Korea, China and Iran.

Introduction

The current threat of chemical and biological warfare can be examined by first assessing countries that have or are seeking a chemical and biological weapons capability. Among the countries who have the capability, assessing the intention of countries and willingness to use these weapons in relation to their strategic objectives will help elucidate this particular threat. Additionally, the status and advancements of the biotechnology industry and each countries' infrastructure, the existing defense measures against current chemical and biological agents, and the effectiveness of the Conventions and the Australia Group (AG) also contribute to the assessment of this threat.

Biological warfare agents are deliberately released microorganisms or microorganism-based toxins, that cause diseases in humans, animals or plants⁴⁴⁰. A majority of biological agents that are used in warfare cause similar or indistinguishable conditions/symptoms from those of naturally occurring diseases, contributing to the difficulty of identifying a biological attack. The Center for Disease Control and Prevention (CDC) has separated biological agents into three categories based on its ease of dissemination and its mortality rate⁴⁴¹. Despite the plethora of naturally occurring bacteria, viruses and toxins, only a small number of these are effective as weapons in a military context. The utility of an agent is based on the ease of production, stability of the agent in storage and in weapon devices, and the infectivity or toxicity⁴⁴².

Chemical warfare agents are man-made, chemical substances that are deliberately used in order to cause major harm, incapacitate, or kill by

⁴⁴⁰ Duraipandian Thavaselvam and Rajagopalan Vijayaraghavan. "Biological Warfare Agents". *J Pharm Bioallied Sci*, Jul-Sep 2010: 179–188. doi: 10.4103/0975-7406.68499.

⁴⁴¹ "Preparedness Home: Biological Weapons", John Hopkins Bloomberg School of Public Health, accessed August 6, 2020, https://www.jhsph.edu/research/centers-and-institutes/johns-hopkins-center-for-public-health-preparedness/tips/topics/Biologic_Weapons/BioWeapons.html.

⁴⁴² Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*. Office of the Surgeon General, Department of the Army, United States of America, 1997. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.8260&rep=rep1&type=pdf#page=24>.

its physiological effects⁴⁴³. Toxic substances have been characterized as chemical warfare agents based on characteristics such as high potency, high toxicity, and persistency⁴⁴⁴. Whether an agent is persistent or non-persistent is directly related to the volatility of the agent, in that agents with high volatility evaporate and disperse more rapidly⁴⁴⁵. The main categories of chemical agents are nerve agents, vesicants, choking agents, blood agents, and riot-control agents (incapacitants)^{446, 447}. Nerve agents affect the functionality of the human nervous system by inhibiting the enzyme acetylcholinesterase (AChE). Vesicants are agents that produce blisters (vesicles) on the skin in addition to potential effects on the upper respiratory tract and the eyes⁴⁴⁸. Blood agents disrupt the typical processes of our body tissues' oxygen consumption and inhibit particular enzymes⁴⁴⁹. Choking agents primarily cause damage to the respiratory tract, particularly the lungs, and asphyxiation⁴⁵⁰. Riot control agents cause incapacitation by irritating the eyes and upper respiratory tract but they do not have permanent effects⁴⁵¹. Chemical warfare agents are also found in the civilian sector as these chemicals are used industrially and manufactured for other peaceful purposes, and thus giving an opportunity for countries to effectively conceal harmful intent.

⁴⁴³ The Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense. Chemical and Biological Defense Primer, Department of Defense, October 2001. Accessed August 6, 2020. <https://www.hsdl.org/?view&did=1504>.

⁴⁴⁴ K Ganesan, S.K. Raza, and R. Vijayaraghavan. "Chemical Warfare Agents". *J Pharm Bioallied Sci*, Jul-Sep 2010: 166–178. doi: 10.4103/0975-7406.68498.

⁴⁴⁵ Ganesan, Raza, Vijayaraghavan, "Chemical Warfare Agents".

⁴⁴⁶ Ibid.

⁴⁴⁷ Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*, 1997.

⁴⁴⁸ Ibid.

⁴⁴⁹ Ganesan, Raza, Vijayaraghavan, "Chemical Warfare Agents".

⁴⁵⁰ Ibid.

⁴⁵¹ Ibid.

History of Biological and Chemical Weapons

Although toxic chemical substances and bacteria/viruses have been weaponized for a long time, chemical and biological warfare between countries during World War I was a catalyst for the modern development and knowledge of these weapons. Table 1 expresses the presence of chemical or biological warfare in major international conflict. This table does not cover all conflicts or other isolated instances of chemical/biological weapon use. Throughout the assessment of chemical and biological warfare attacks, it can be difficult to confirm whether the malign effects were due to a natural or a deliberate source. Therefore, the term ‘alleged’ expresses that there is not absolute certainty that it was a chemical or biological weapon but there is either substantial or sufficient evidence to believe so.

Table 1. Chemical and Biological Weapon Presence in Major International Conflict

Conflict	Description	Aggressor: Agent	Impact of Agent	Validity (Alleged or Confirmed)
World War I ⁴⁵²	After the assassination of Archduke Franz Ferdinand, Austria declared war on Serbia. Due to alliances, Austria-Hungary, Germany and Italy (the Triple Alliance) opposed Great Britain, France, and Russia (the Triple Entente)	<ul style="list-style-type: none"> German: chlorine gas, phosgene, diphosgene, chloropicrin British: chlorine French: chlorine, hydrogen cyanide, cyanogen chloride, mustard 	<ul style="list-style-type: none"> 1 million out of 26 million casualties suffered by all nations were from gas 	Confirmed
Italian-Ethiopian War 1935 ⁴⁵³	Benito Mussolini launched invasion of Ethiopia	<ul style="list-style-type: none"> Italy: sulphur mustard bombs and sprayed from airplane tanks 	<ul style="list-style-type: none"> Effective due to Ethiopian soldier's open military uniform Strategic effect on Italy's success and demoralizing Ethiopian forces 	Confirmed

⁴⁵² Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*, 1997.

⁴⁵³ Lina Grip and John Hart. *The use of chemical weapons in the 1935–36 Italo-Ethiopian War*. SIPRI Arms Control and Non-proliferation Programme, October 2009. Accessed August 8, 2020. <https://www.sipri.org/sites/default/files/Italo-Ethiopian-war.pdf>.

Sino-Japanese war 1937 ⁴⁵⁴	During Japan's large-scale invasion of China, the Japanese deployed chemical weapons and used bioagents in experiments on Chinese prisoners of war	<ul style="list-style-type: none"> Japan: vomiting agents, blistering agents -Japan: biological agents used in experiments with Unit 731 	<ul style="list-style-type: none"> Helped achieve military objectives Japan's Unit 731 experiments are considered a war crime 	Confirmed
Vietnam War ⁴⁵⁵	Conflict between communist North Vietnam and South Vietnam and their allies	US: Agent Orange (tactical herbicide) Vietnam: herbicides	<ul style="list-style-type: none"> Immediate environmental effects/destroy food supply Long-term health problems for Vietnamese people and US Veterans 	Confirmed
Egypt intervention in Yemeni civil war 1963 ⁴⁵⁶	Egyptian military support of the revolutionists that overthrew Yemen's monarch, Imam Muhammad al-Badr	Egypt: mustard gas, tear gas (CN), phosgene asphyxiant	<ul style="list-style-type: none"> Egyptian President Gamal Abdel Nasser's military gas bombings allowed free reign in Yemen 	Confirmed
Iraq-Iran War ⁴⁵⁷	Iraq invaded Iran	Iraq: mixture of mustard gas and nerve agent tabun Iran: cyanide	<ul style="list-style-type: none"> Significant element for Iraq in achieving tactical battlefield objectives 	Confirmed
Persian Gulf War ⁴⁵⁸	Iraq invasion of Kuwait. Coalition member countries involvement.	No use of unconventional weapons within the war. After the war: Khamsiyah Pit nerve agent release at low levels	Persian Gulf War syndrome – US soldiers who were deployed experienced wide ranging symptoms	Alleged

⁴⁵⁴ Ping Bu, "A research report on Japanese use of chemical weapons during the Second World War". *Journal of Modern Chinese History*, vol. 2, June 2010: 155–172. <https://doi.org/10.1080/17535650701677239>.

⁴⁵⁵ Greg Goebel, "A History of Chemical & Biological Warfare", Accessed August 11, 2020. https://www.cia.gov/library/abbottabad-compound/65/65A3FAC0A645BA2C3FAC8C187499C16D_the_history_of_chemical_war_fare.pdf.

⁴⁵⁶ Asher Orkaby "Forgotten Gas Attacks in Yemen Haunt Syria Crisis". Accessed August 11, 2020. <https://wcfia.harvard.edu/publications/forgotten-gas-attacks-yemen-haunt-syria-crisis>.

⁴⁵⁷ Javed Ali. "Chemical Weapons and the Iran-Iraq War: A Case Study in Noncompliance" *The Nonproliferation Review*/Spring, 2001, Accessed August 11, 2020. <https://www.nonproliferation.org/wp-content/uploads/npr/81ali.pdf>.

⁴⁵⁸ Persian Gulf War Illnesses Task Force. "Intelligence Update: Chemical Warfare Agent Issues During the Persian Gulf War". April 2002. Accessed August 11, 2020. <https://www.hsd.org/?view&did=2796>.

Conflict	Description	Aggressor: Agent	Impact of Agent	Validity (Alleged or Confirmed)
Soviet Union in Afghanistan/ Southeast Asia ⁴⁵⁹	Soviet Union provided chemical warfare agents to forces in Laos, Kampuchea, Afghanistan	<ul style="list-style-type: none"> Soviet backed Lao and Vietnamese forces: trichothecene mycotoxins Soviet forces in Afghanistan: lethal and nonlethal agents 	<ul style="list-style-type: none"> Effective way to demoralize and fight the resistance of anti-government forces 	Alleged but Substantive Evidence (Yellow rain controversy)
Syrian Civil War ⁴⁶⁰	President Bashar al-Assad fight against the insurgency, coalition efforts to defeat Islamic State	Syrian government: chlorine, sarin	<ul style="list-style-type: none"> Large number of civilian casualties 	Confirmed

The table shows a tendency for state actors to use chemical weapons rather than biological weapon use in warfare, aside from Soviet-supplemented toxins in Laos and Vietnam. This trend indicates that the development and exploitation of chemical weapons occurred much faster in comparison to biological weapons. Moreover, during the Persian Gulf War, Iraq did not use chemical weapons against opposing forces. However, many Gulf War veterans experienced a myriad of symptoms and conditions that have no source or explanation. Although there is no method to definitively identify the source of these symptoms, the Department of Defense (DoD) has concluded that these veterans might have been exposed to low-levels of nerve agents due to the demolition of chemical agents in Khamisiyah⁴⁶¹.

⁴⁵⁹ Alexander M. Haig. "Chemical Warfare in Southeast Asia and Afghanistan". United States Department of State, 1982. Accessed August 11, 2020. <https://www.cia.gov/library/readingroom/docs/CIA-RDP97M00248R000500010018-6.pdf>.

⁴⁶⁰ Gregory D. Koblentz. "Chemical-weapon use in Syria: atrocities, attribution, and accountability". *The Nonproliferation Review*, vol. 26, February 2020: 575–598. <https://doi.org/10.1080/10736700.2019.1718336>.

⁴⁶¹ U.S. Department of Veterans Affairs. "Chemical and Biological Weapons during Gulf War". Accessed August 12, 2020. <https://www.publichealth.va.gov/exposures/gulfwar/sources/chem-bio-weapons.asp>.

During WWI, Germans attempted to spread diseases such as anthrax, cholera and glanders in animals, but the attempts proved unsuccessful⁴⁶². Around the time of World War II, many countries were arguing over disputed claims of experimentation with biological warfare agents. Many of these allegations deal with Japanese use of biological agents against the Soviet Union and China⁴⁶³. Although not used in combat, during the entirety of WWII, Japan conducted extensive biological warfare experiments in multiple facilities, collectively known as Unit 731, in which thousands of prisoners of war were experimented on with biological agents⁴⁶⁴. Germany also conducted similar experiments on prisoners, but they diverged from Unit 731's great brutality⁴⁶⁵. The Japanese biological weapon research included agents causing plague, typhoid and typhus⁴⁶⁶. Although many allegations of biological weapon use existed during that time, a majority of them lacked sufficient scientific evidence to support it. Allegations involved countries with a biological weapon capability such as Great Britain, U.S., Germany and North Korea⁴⁶⁷.

In 1979, a Soviet Union facility that was openly used for industrial purposes, exploded and accidentally released anthrax, raising suspicion on previous Soviet claims of halting their offensive biological weapons program in the 1960s⁴⁶⁸. By 1989, it was revealed that an extensive biological warfare program, named Biopreparat, had been operating since 1973⁴⁶⁹.

⁴⁶² Frischknecht, Friedrich. "The history of biological warfare". *EMBO Rep*, June 2003: S47–S52. doi: 10.1038/sj.embor.embor849.

⁴⁶³ Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*, 1997.

⁴⁶⁴ Howard Brody et al. "U.S. responses to Japanese wartime inhuman experimentation after World War II". *Camb Q Healthc Ethics*, April 2014: 220–230. doi: 10.1017/S0963180113000753.

⁴⁶⁵ Ibid.

⁴⁶⁶ Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*, 1997.

⁴⁶⁷ Ibid.

⁴⁶⁸ Sahl, Jason W. et al. "A *Bacillus anthracis* Genome Sequence from the Sverdlovsk 1979 Autopsy Specimens. Accessed August 12, 2020. <https://mbio.asm.org/content/7/5/e01501-16>.

⁴⁶⁹ Hoffman, David E. "Cracking open the Soviet biological weapons system, 1990". The National Security Archive, 2009. Accessed August 12, 2020. <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB315/index.htm>.

Soviet leaders initially attributed the anthrax outbreak to the ingestion of contaminated animal products until admitting its sinister background in 1992. The Soviet Union also provided technology to the Bulgarian state security in 1978 to aid in an assassination attempt of Georgi Markov, with a pellet that contained toxin ricin⁴⁷⁰. Moreover, although Saddam Hussein did not use biological or chemical weapons in the Persian Gulf War, Iraq had an extensive offensive biological warfare capability⁴⁷¹.

Conventions/Treaties and their Effectiveness

The use of chemical and biological weapons instigated international outcry in many instances due to their high communicability, high mortality, and demoralizing impact on troops. Therefore, after repeated major use in international conflict, various methods were implemented to control and monitor the production and use of chemical and biological weapons.

The “Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare”, known as the 1925 Geneva Protocol, was the first major international treaty that prohibits the use of chemical and biological weapons. Due to the large chemical use in World War I, the prohibition was initially addressed only for the use of toxic gases in war but was later extended to the use of “bacteriological methods of warfare”⁴⁷². The progression reflects the increased prominence of chemical warfare over biological warfare in history. Iraq violated the protocol during the Gulf War, and Italy violated it during the Italian-Ethiopian War, suggesting the treaty’s ineffectiveness⁴⁷³.

⁴⁷⁰ Nehring, Christopher. “Umbrella or pen? The murder of Georgi Markov. New facts and old questions”. *Journal of Intelligence History*, February 2016: 47–58. <https://doi.org/10.1080/16161262.2016.1258248>.

⁴⁷¹ Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*, 1997.

⁴⁷² Bureau of International Security and Nonproliferation. *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (Geneva Protocol)*, June 1925. Accessed August 13, 2020. <https://2009-2017.state.gov/t/isn/4784.htm#treaty>.

⁴⁷³ Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*, 1997.

To complement the Geneva Protocol, along with the increased research and development of biological weapons during World War II, the 1972 “Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction”, or the Biological Weapons Convention (BWC), went into effect in March 1975⁴⁷⁴. Parties within the Convention are prohibited from developing any biological agents or toxins in quantities beyond peaceful or civilian uses. The treaty also addresses that members should not aid anyone to produce these agents. The effectiveness of this convention is questioned due to the lack of verification methods to assure that countries are following the convention’s principles and the lack of compliance of certain countries (such as the Soviet Union)⁴⁷⁵. The Convention on the Prohibition of the Development, Production, Stockpiling, and Use of Chemical Weapons and on their Destruction, known as the 1993 Chemical Weapons Convention (CWC), is a treaty that prohibits developing, transferring, and use of chemical weapons⁴⁷⁶. The Organization for the Prohibition of Chemical Weapons (OPCW) implements the principles stated in the treaty and assesses members related activities and declarations. Due to the OPCW, the proliferation of chemical weapon use is likely more contained.

After the discovery of Biopreparat and Russia’s ability to keep it hidden for a long time, Russia agreed to a Trilateral Agreement with the US and UK in order to quell fear and worries about Russia’s dishonesty with dismantling its biological weapons programs⁴⁷⁷. However, Russia has failed to maintain this agreement, thus little concrete information exists about their current

⁴⁷⁴ U.S. Department of State. “Biological Weapons Convention”. Accessed August 13, 2020. <https://www.state.gov/biological-weapons-convention/>.

⁴⁷⁵ Rissanen, Jenni. “The Biological Weapons Convention”. Nuclear Threat Initiative, March 2003. Accessed August 13, 2020. <https://www.nti.org/analysis/articles/biological-weapons-convention/>.

⁴⁷⁶ Kimball, Daryl G. “The Chemical Weapons Convention (CWC) at a Glance”. Arms Control Association, April 2020. Accessed August 13, 2020. <https://www.armscontrol.org/factsheets/cwcglance>.

⁴⁷⁷ Moodie, Michael. “The Soviet Union, Russia, and the Biological and Toxin Weapons Convention”. *The Nonproliferation Review/Spring 2001*, Accessed August 13, 2020. <https://www.nonproliferation.org/wp-content/uploads/npr/81moodie.pdf>.

biological related facilities and organizations⁴⁷⁸. Due to the discovery that the international chemical industry largely contributed to Iran’s chemical warfare program (implemented in the Iran-Iraq war), The Australia Group (AG) was established in 1985 as an informal group of countries aimed to enforce export controls to prevent the proliferation of chemical and biological weapons⁴⁷⁹. The organization has a list of items to monitor including chemical weapon precursors, dual-use equipment for both types of weapons, and biological agents/organisms⁴⁸⁰.

The discovery of these two countries maintaining their offensive capabilities proves that these conventions and agreements have not been successful in completely deterring the use of these weapons, of which is also partly due to the fact that some countries in the world have never signed the agreement. The international community must work together to identify those violating the agreements and condemning or punishing those that use chemical and biological weapons.

Biological and Chemical Agents and Their Defense

Main Chemical Agents⁴⁸¹

Nerve Agents:	Tabun (GA), Sarin (GB), Soman (GD)
Vesicants:	sulfur mustard, lewisites
Blood agents:	Hydrogen cyanide (HCN), cyanogen chloride (CNCl)
Choking agents:	Chlorine, phosgene
Incapacitating:	BZ (3-quinuclidinyl benzilate)

⁴⁷⁸ Zilinskas, Raymond A. “The Soviet Biological Weapons Program and Its Legacy in Today’s Russia”. National Defense University, July 2016. Accessed August 14, 2020. https://inss.ndu.edu/Portals/68/Documents/occasional/cswmd/CSWMD_OccasionalPaper-11.pdf?ver=2016-07-18-144946-743.

⁴⁷⁹ Nuclear Threat Initiative. “Australia Group (GA)”. Accessed August 14, 2020. <https://www.nti.org/learn/treaties-and-regimes/australia-group-ag/>.

⁴⁸⁰ Ibid.

⁴⁸¹ Ganesan, Raza, Vijayaraghavan, “Chemical Warfare Agents”.

Main Biological Agents⁴⁸²

Bacteria:	<i>Bacillus anthracis</i> (anthrax), <i>Yersinia pestis</i> (plague), <i>Francisella tularensis</i> (tularemia), <i>Brucella</i> species (brucellosis) <i>Coxiella burnetti</i> (Q fever)
Viruses:	Variola virus (smallpox), Equine encephalitis viruses, virus-based hemorrhagic fevers
Toxins:	Staphylococcal enterotoxin B, Ricin, Botulinum toxins, Trichothecene mycotoxins

The Impact of the Biotechnology Industry

Due to the fact nearly all of the information, research facilities, and equipment/supplies necessary for biological weapons are also used in peaceful and civilian interests, countries with advanced biotechnology sectors have the potential to discreetly develop advanced biological weapon capability⁴⁸³. However not only do advancements in biotechnology provide greater opportunity for more lethal weapons, but it also allows advancements in defense countermeasure programs for these weapons.

After the mid-1970s, scientists began mastering the use of biotechnology and the manipulation of DNA to the extent to which the scientific community acquired the ability to sequence the entire human genome⁴⁸⁴. Following the natural progression cycle of new products, biotechnology started to become commercialized and has grown into a vast industry. The increased availability of biotechnology and advancements in knowledge in the industry also simultaneously increases the likelihood of this technology landing in the hands of a person with malevolent intentions. For example, through various experiments with these technologies, humans have gained the

⁴⁸² Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*, 1997.

⁴⁸³ Zilinskas, Raymond A. "Second-Tier Suppliers of Biological Warfare Technology, Equipment, and Materials: The Potential Roles of China, India, and Cuba". James Martin Center for Nonproliferation Studies, January 2008. Accessed August, 14, 2020. <https://www.hsdl.org/?view&did=716634>.

⁴⁸⁴ Gadagkar, Raghavendra. "Chapter: 4 The Biotechnology Revolution: Exploring New Territory Together". *Sciences Engineering Medicine*, 2016. Accessed August 14, 2020. <https://www.nap.edu/read/21810/chapter/7>.

ability to purposefully make pathogens more severe (virulent)⁴⁸⁵. Generally, understanding the capabilities offered by biotechnology to manipulate genes is important to help prepare for the different ways adversaries might enhance biological agents to cause more harm or defy current defense mechanisms.

Existing Defense Measures

The existence of effective and available medical countermeasures could potentially serve as a deterrent to use these weapons, in which the difficulties to stabilize and deploy the weapons is not worth the potential of an ineffective outcome. A defense capability against chemicals and toxins exist through physical countermeasures such as protective masks and clothing, decontamination, and vaccines⁴⁸⁶. Additionally, detection systems for chemical and biological agents exist such as handheld devices, bio surveillance and wide-area detection which immensely increase the likelihood for soldiers to avoid casualties⁴⁸⁷. Defense against an attack with these weapons is more effective when there is awareness of enemy intentions, training with the equipment, and sufficient amounts of equipment⁴⁸⁸. Although defense measures against these weapons exist, it is often hard to decipher an actors' intentions and the extent of their capability.

⁴⁸⁵ Raghavendra Gadagkar, "Chapter: 4 The Biotechnology Revolution: Exploring New Territory Together".

⁴⁸⁶ Frederick R. Sidell, Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*, 1997.

⁴⁸⁷ United States Air Force Center for Unconventional Weapons Studies. *Chemical and Biological Warfare Overview*. Accessed August 14, 2020. <https://www.airuniversity.af.edu/Portals/10/CSDS/Books/cbwprimer2015.pdf>.

⁴⁸⁸ Ibid.

State Actors with Capability/Intentions

Russia

Due to the use of chemical weapons during World War I, the government in the former Soviet Union focused on growing a chemical industry for military and civilian purposes. By the late 1920's, leaders such as Yakov M. Fishman were focused on pursuing a biological capability⁴⁸⁹. After the creation of the first biological weapon laboratory called the Scientific Research Institute of Health led by Nikolay N. Ginsburg, many others were established to research other infectious diseases and develop vaccines against such diseases⁴⁹⁰. By World War II, the Soviet Union's offensive biological weapons programs was vast. Despite the United States' public dismantling of its offensive biological weapons program in 1969, and the Soviet's signing of the Biological Weapons Convention in 1972, the Soviet Union's offensive biological weapons programs continued—its existence was only disclosed publicly in 1989⁴⁹¹. The undisclosed nature of the Soviet's biological weapons capability was likely a part of the very reason why the Soviet's continued maintaining and advancing it, as it would serve as a major surprise in a potential future scenario. Thus, the Soviet Union had an extensive biotechnology industry intended to weaponize biological agents, often masked as civilian institutions such as Biopreparat⁴⁹².

Although Russia's former president Boris Yeltsin admitted the Soviet's violation of the Biological Weapons Convention throughout the Cold War in 1992, the current Russian president, Vladimir Putin, has reasserted that the Soviet offensive biological warfare capability never existed⁴⁹³. Putin's denial of the Soviet program suggests that Russia's current leaders also

⁴⁸⁹ Raymond A Zilinskas, "The Soviet Biological Weapons Program and Its Legacy in Today's Russia".

⁴⁹⁰ Ibid.

⁴⁹¹ Ibid.

⁴⁹² Ibid.

⁴⁹³ Trakimavicius, Lukas. "Is Russia Violating the Biological Weapons Convention". Atlantic Council, May 2018. <https://www.atlanticcouncil.org/blogs/new-atlanticist/is-russia-violating-the-biological-weapons-convention/>.

have a tendency to conceal the truth. After the failure of the Trilateral agreement between Russia, the U.S. and the U.K. in 1992, whether the Soviet program was actually dismantled, in which all pathogens have been destroyed, is unclear. Given a long history of secrecy and extensive capability, it is likely that Russia inherited much of the knowledge and weapons of the previous Soviet biological warfare program.

According to a 2012 article by Vladimir Putin in the *Rossiiskaya Gazeta*, Russia's military will develop weapons systems "based on new principles such as beam, geophysical, wave, genetic, psychophysical and other technology", proving that there is an interest in unconventional warfare weapons and tactics to achieve their strategic goals⁴⁹⁴. Particularly, President Putin's eagerness to create new weapons based on 'genetic' principles flashes warning signs of the production of biological weapons in violation of the BWC. Additionally, there has been no indication that Russia has reduced its biological facilities that were previously used for the Soviet offensive capability⁴⁹⁵. Therefore, although not proven, it is reasonable to assess that Russia likely has the ability to maintain an offensive biological weapons program and will be willing to use biological weapons in future war scenarios, if given the correct opportunity.

Regarding chemical weapons, Russia's production of chemical agents and weapons was the most extensive during World War II⁴⁹⁶. However, after becoming a member of the 1993 Chemical Weapons Convention, Russia committed to destroy all its declared chemical weapon stockpiles⁴⁹⁷. By October 2017, the OPCW declared that Russia had destroyed 39,967 metric tons of chemical weapons, which serves as 96.3 percent of its stockpiles⁴⁹⁸.

⁴⁹⁴ Putin, Vladimir. "Being strong: National security guarantees for Russia". *Rossiiskaya Gazeta*, February 2012. Accessed August 15, 2020. <http://archive.premier.gov.ru/eng/events/news/18185/>.

⁴⁹⁵ Raymond A Zilinskas, "Second-Tier Suppliers of Biological Warfare Technology, Equipment, and Materials: The Potential Roles of China, India, and Cuba".

⁴⁹⁶ Federation of American Scientists. "Chemical Weapons". Accessed August 15, 2020. <https://fas.org/nuke/guide/russia/cbw/cw.htm>.

⁴⁹⁷ Ibid.

⁴⁹⁸ OPCW News. "OPCW Marks Completion of Destruction of Russian Chemical Weapons Stockpile". October 2017. Accessed August 15, 2020. <https://www.opcw.org/media-centre/news/2017/10/opcw-marks-completion-destruction-russian-chemical-weapons-stockpile>.

However, in 2018, Russia used the nerve agent Novichok to attempt to assassinate a former Russian spy Sergei Skripal, demonstrating their violation of the CWC⁴⁹⁹. Therefore, it is uncertain whether Russia has truly dismantled their chemical weapon capability.

Syria

Syria focused on developing a chemical weapons program primarily due to the military aggression of Israel in the Middle East, exemplified in Israel's invasion of Lebanon in 1982⁵⁰⁰. Syria's chemical weapon capability serves as a deterrent tactic against the Israeli threat and provides a method to counterbalance the disparity between their militaries. Evidence exists that suggest that the Soviet Union and other countries aided in the development of their capability⁵⁰¹. Official U.S. assessments in 2013 indicated that Syria had 1,000 metrics tons of chemical agent stockpiles that consisted of mustard, sarin, and VX nerve agents⁵⁰². Due to the violence of the Syrian civil war starting in 2011, there have been many alleged chemical attacks between 2012–2013⁵⁰³. However, most of the early alleged incidences had low casualties, contrasting from the confirmed, large chemical attack against Ghouta using the sarin nerve agent⁵⁰⁴. Therefore, Syria is an example of a country in which the existence of their chemical weapons capability is rooted out of defense against aggressors (in the Middle East), yet they have been exercising it offensively without a 'first-use' from another country. Although the Syrian government used these agents against their own civilian population and not against another country, this type of warfare in general is unacceptable.

⁴⁹⁹ Coats, Daniel R. *Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, January 2019. Accessed August 15, 2020. <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.

⁵⁰⁰ Mauroni, Albert J. *Eliminating Syria's Chemical Weapons*. US Air Force Center for Unconventional Weapons Studies, Future Warfare Series, No. 58. June 2017. Accessed August 16, 2020. <https://media.defense.gov/2019/Apr/11/2002115522/-1/-1/0/58ELIMINATINGSYRIACW.PDF>.

⁵⁰¹ Ibid.

⁵⁰² Ibid.

⁵⁰³ Ibid.

⁵⁰⁴ Ibid.

Due to pressure from the U.S., Syria acceded to the Chemical Weapons Convention and thereby committed to destroying its chemical weapons stockpiles. Despite the fact that the OPCW declaration of the destruction of all of Syria's declared chemical weapon stockpiles in 2015, there have been alleged Syrian military use of agents in 2016 and 2017⁵⁰⁵. Therefore, despite efforts from the international community, Syria has the capability and intent to use chemical weapons. Contrastingly, little information exists about Syria potentially having a biological weapons capability.

North Korea

North Korea's potential chemical and biological warfare capabilities have been disputed due to the fact that very little information is known about their programs or intentions, if any exist⁵⁰⁶. However, there is reason to believe that North Korea has a chemical weapons capability contrasting from their biological weapons capability, which remains largely unknown or unconfirmed. Recently in 2017, North Korea supported the murder of Kim Jong-Un's half-brother Kim Jong-Nam, with a form of VX nerve agent in an airport in Malaysia⁵⁰⁷. The fact that this assassination was in a public place such as an airport, indicates that the North Korea wanted a large audience to witness the assassination. Based on this incident, North Korea might have some sort of chemical weapons capability or knowledge about agents and is willing to use it to complete strategic objectives.

Based on the technical knowledge to develop its nuclear missile programs, it is possible for North Korea to create these other unconventional weapons⁵⁰⁸. Additionally, North Korea has a sufficient biotechnol-

⁵⁰⁵ Albert J Mauroni, *Eliminating Syria's Chemical Weapons*.

⁵⁰⁶ Parachini, John V. "North Korea's CBW Program: How to Contend with Imperfectly Understood Capabilities". RAND Santa Monica United States, 2018. Accessed August 16, 2020. <https://apps.dtic.mil/sti/pdfs/AD1056014.pdf>.

⁵⁰⁷ Daniel R Coats, *Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, January 2019.

⁵⁰⁸ Parachini, John V. "North Korea's CBW Program: How to Contend with Imperfectly Understood Capabilities".

ogy industry in order to maintain a biological weapons capability⁵⁰⁹. For example, the Pyongyang Bio-technical Institute, a pesticide production facility, has been scrutinized as a possible dual-use facility⁵¹⁰. Although this facility is operating under peaceful purposes, it is important to acknowledge that there is potential for biological weapon weapons to be produced there. South Korea's 2015 White Paper's have stated that North Korea has over thirteen types of biological agents and the capability to weaponize them⁵¹¹. These claims have not been substantiated by other sources, but the lack of confirmation of this information should not invite complacency by assuming that North Korea does not possess a capability. The international community should at least imagine the worst-case scenario and assess how to best prepare for such a scenario.

China

China's biological weapon's research and development activities abide by the Biological Weapons Convention, because it is ostensibly intended for defensive purposes⁵¹². Although China had created an active offensive biological weapons program in the mid 1970s, China became a member of the BWC in 1984.

However, suspicion of the existence of a Chinese offensive biological weapon program grew after assessing that the Chinese military controlled a few of the biological research centers intended for civilian purposes in 1993⁵¹³.

⁵⁰⁹ Coats, Daniel R. *Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, February 2018. Accessed August 16, 2020. <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>.

⁵¹⁰ Kim, Hyun-Kyung, Elizabeth Philipp, and Hattie Chung. "North Korea's Biological Weapons Program: The Known and Unknown. *HARVARD Kennedy School, Belfer Center for Science and International Affairs*, October 2017. <https://www.belfercenter.org/sites/default/files/2017-10/North%20Korea%20Biological%20Weapons%20Program.pdf>.

⁵¹¹ Hyun-Kyung Kim, Elizabeth Philipp, and Hattie Chung. "North Korea's Biological Weapons Program: The Known and Unknown."

⁵¹² Shoham, Dany. "China's Biological Warfare Programme: An Integrative Study with Special Reference to Biological Weapons Capabilities". *Journal of Defence Studies*, 2015: 131–156. Accessed August 16, 2020. https://idsa.in/system/files/jds/jds_9_2_2015_DanyShoham.pdf.

⁵¹³ Dany Shoham, "China's Biological Warfare Programme: An Integrative Study with Special Reference to Biological Weapons Capabilities".

Additionally, a major facility for researching biotechnology and genetic engineering stopped publishing information in 2001 yet remained active as a facility⁵¹⁴. These activities suggest that China is trying to keep portions of their biological research/defense programs secretive. Based on the plethora of facilities that research biological products and other related activities that reside in China, and specifically those that are affiliated with the PLA or government-based defense organizations, China has the capability necessary to mass produce biological weapons and create an advanced offensive biological warfare program⁵¹⁵. China's massive biotechnology industry and infrastructure allows opportunity for the creation of a biological weapons capability that could be hidden from the international community due to the fact that facilities and research can be considered dual-use. Despite China's ability to obtain the weapons capability, China is likely to be cautious in using them in an international conflict as they hold status of major global power in the international community. However, based on history, China has no issue with violating human rights and going great lengths in order to reach their strategic goals.

After adhering to the CWC principles and dismantling their offensive chemical weapon capability, China has officially stated that they continue a chemical warfare program for defensive and protection purposes⁵¹⁶. Instead of participating in the AG, China has attempted to develop and implement its own export controls for chemical weapons, but implementation and reinforcement of this domestically run program has proven difficult⁵¹⁷. The fact that China's export controls is not under supervision of an outside source allows these activities to remain ambiguous and allows public knowledge of China's chemical-related exports to remain controlled and small.

China's defense programs for biological and chemical weapons requires research and knowledge of agents and their weaponization/dissemination,

⁵¹⁴ Ibid.

⁵¹⁵ Ibid.

⁵¹⁶ Nuclear Threat Initiative. "Countries: China". Accessed August 16, 2020. <https://www.nti.org/learn/countries/china/chemical/>.

⁵¹⁷ Ibid.

thus it is plausible to assess that China could harness an advanced capability in both areas if needed in a wartime contingency.

Iran

The Iraqi chemical weapon use in the Iraq-Iran War (1980–1988) prompted Iran to develop a chemical weapons capability⁵¹⁸. As Iran gained the ability to manufacture, weaponize and deploy chemical agents during the war, it became more difficult to identify the perpetrator of the different chemical attacks in the war⁵¹⁹. After the war, Iran claimed that its chemical weapon program was dismantled and joined the CWC in 1997⁵²⁰. However, there have been many allegations of Iran maintaining their chemical weapons capability. Countries such as India and China have sold significant amounts of chemical weapons materials to Iran and significantly advanced Iran's chemical weapon infrastructure⁵²¹. This prompted the U.S. to pass the Iran Nonproliferation Act and impose sanctions on these countries. Recent U.S. official documents express concern that Iran is not fulfilling its obligations under the CWC by continuing to develop offensive chemical agents and failing to declare all of its capabilities⁵²².

Iran's advanced civilian biotechnology sector has the potential use the dual-use supplies and equipment to contribute to offensive military purposes⁵²³. Iran has focused on researching and developing vaccines, researching agricultural biotechnology and different dissemination techniques

⁵¹⁸ Federation of American Scientists. "Iranian NBC Policy, Capabilities, and Employment Options". Denial and Jeopardy: Deterring Iranian Use of NBC Weapons. Accessed August 16, 2020. <https://fas.org/nuke/guide/iran/doctrine/dajd/ch5.html>.

⁵¹⁹ Iran Watch. "A History of Iran's Chemical Weapon-Related Efforts". Wisconsin Project on Nuclear Arms Control, November 2019. Accessed August 16, 2020. <https://www.iranwatch.org/our-publications/weapon-program-background-report/history-irans-chemical-weapon-related-efforts>.

⁵²⁰ Nuclear Threat Initiative. "Countries: Iran: Chemical". Accessed August 16, 2020. <https://www.nti.org/learn/countries/iran/chemical/>.

⁵²¹ Ibid.

⁵²² Daniel R Coats, *Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, January 2019.

⁵²³ Nuclear Threat Initiative. "Countries: Iran: Biological". Accessed August 16, 2020. <https://www.nti.org/learn/countries/iran/biological/>.

for plant pesticides⁵²⁴. Iran also continues to research into microbiology and genetic engineering at health research facilities, exemplifying their expertise and knowledge in the field. Overall, the dual-use nature of these facilities and this biological research, indicates that Iran is able to create a biological weapons capability effectively and quickly, if they do not have a clandestine one already.

Nonstate Actors – Biological and Chemical based Terrorism

Terrorists have acquired and deployed biological weapons on many accounts, of which primarily target civilians⁵²⁵. U.S. law enforcement prevented two attempts of infection with biological agents in America, including an attempt in 1972 by two college students in Chicago, and another attempt by the Bhagwan Shree Rajneesh followers in Oregon⁵²⁶. The perpetrators of these attempts show the broad spectrum of people that have sought to use these types of weapons.

More internationally recognized cases of bioterrorism include the Russia-sponsored Aum Shinrikyo Japanese religious group release of anthrax in Tokyo and the 2001 anthrax infested mail attacks against news media and US Congress⁵²⁷. Moreover, ISIS has used chemical weapons such as mustard and other toxic substances in Syria and Iraq multiple times throughout 2014–2017⁵²⁸. Due to increased availability and knowledge of chemical and biological weapons, terrorists are more likely to acquire this capability.

⁵²⁴ Ibid.

⁵²⁵ Williams, Mollie and Daniel C. Sizemore. "Biologic, Chemical, and Radiation Terrorism Review". *StatPearls [Internet]*, February 2020. Accessed August 16, 2020. <https://www.ncbi.nlm.nih.gov/books/NBK493217/>.

⁵²⁶ Ibid.

⁵²⁷ Ibid.

⁵²⁸ Daniel R Coats, *Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, January 2019.

Conclusion

Due to the proliferation of chemical and biological weapons and the intentions of the countries that possess these capabilities, the advancements in biotechnology and its dual-use nature of civilian and military purposes, and the decreased effectiveness of international treaties, chemical and biological warfare poses a prominent threat to the international community in the future. The monitoring of export controls, verifications of international agreements, potential sanctions of transporting biological/chemical materials, and advancing defense countermeasures will help deter countries or state actors from using these weapons.

The main countries that are underscored to either possess a biological and chemical weapons capability or possess intent to acquire and use them, include Russia, Syria, North Korea, China, and Iran. Although these countries have not publicly declared offensive capabilities and some of the allegations are not yet confirmed, the international community should not allow the lack of information to lead to the assumption that these countries completely do not have these capabilities. Complacency is dangerous because it increases the likelihood for a country to successfully execute a surprise attack and induce more casualties. Instead, the lack of information should incite the international community to continue to monitor these countries activities and increase its efforts to find more information about their intentions and capabilities.

US and EU Counterterrorism Approaches: From Divisive to Convergent?

Andrée WIETOR

Executive summary: This paper attempts to analyze the risks that lie in a military approach to counterterrorism and the development of European Union counterterrorism after 9/11. It describes the immediate responses of the US and the EU to 9/11 and attempts to explain, why they adopted different approaches in the aftermath. Furthermore, it analyzes the reactions to the Paris attacks in 2015 and argues that these attacks, together with the ones perpetrated in 2016, mark a shift in EU counterterrorism. It finally asks whether US and EU approaches to counterterrorism have converged in recent years and what chances and risks this eventual convergence entails.

Keywords: EU counterterrorism, US counterterrorism, terrorism-as-crime, terrorism-as-war, rhetoric, transatlantic divide, transatlantic relations, convergence; EU-US relations

Introduction

The attacks of 9/11 undoubtedly marked a new chapter in the history of terrorism and international politics. The Bush administration did not hesitate to unilaterally launch a military campaign against international terrorism, declaring a “Global War on Terror”, while member states of the European Union were rather in favor of a multilateral and comprehensive

approach in the hope to tackle the root causes of terrorism⁵²⁹. This transatlantic divide led American political scientist Robert Kagan to argue that Americans and Europeans do not share a common strategic culture anymore. In his article “Power and Weakness”, published in 2002, and his bestselling book *Of Paradise and Power: America and Europe in the New World Order*, Kagan claims that Americans are from Mars and cherish an anarchic world view where international law does not exist, while Europeans are from Venus, living in a “post-historical paradise of peace and relative prosperity”⁵³⁰.

Kagan’s controversial representation excludes the possibility of alternative co-existing approaches to terrorism. However, as no policy is perfectly holistic, it might even be necessary to have different approaches that complement each other. Like any other phenomenon in the world, terrorism is constantly changing, and countermeasures must adapt.

Looking at the past 20 years of counterterrorism, it becomes apparent that the success of the US approach was mitigated, and that EU counterterrorism went from hardly relevant to an important and increasingly integrated common policy area. However, when considering the military reaction and rhetoric of the French President after the Paris attacks in 2015, we may wonder if the EU counterterrorism policy is not about to converge with the US approach.

In the present paper, we will first decide on a definition of terrorism and counterterrorism, before analyzing the US and EU approaches to terrorism to assess if there has been a shift in EU policy on terrorism after 2015 and eventually a convergence between US and EU counterterrorism approaches.

⁵²⁹ Pernille Rieker, “Editor’s Introduction”, *Security Dialogue. Special Section: European Security and Transatlantic Relations in the Age of International Terrorism: Challenges for the Nordic Countries* 36, no. 3 (September 2005): 395.

⁵³⁰ Robert Kagan, “Power and Weakness”, *Policy Review* 113 (June/July 2002): 3.

Terrorism and Counter-Terrorism

The definitions of terrorism are numerous and contested, which makes counterterrorism measures equally heterogeneous as our understanding of terrorism determines, which measures we are willing to take to fight it. According to J. Bowyer Bell the “very word [terrorism] becomes a litmus test for dearly held beliefs, so that a brief conversation on terrorist matter with almost anyone reveals a special world view, an interpretation of the nature of man, and a glimpse into a desired future.”⁵³¹. In short, “tell me what you think about terrorism, and I tell you who you are.”⁵³². Hence, it is not surprising that Schmid’s analysis of terrorism definitions reveals that the notion of illegal and criminal actions, the so-called element of opprobrium, is present in 85% of the 88 intergovernmental definitions analyzed, while the same element only reaches 30% in academic definitions. Governments and international organizations are first interested in maintaining order and security, while academics are more interested in the underlying psychological and political elements of terrorism⁵³³.

As I focus my analysis on counterterrorism in the United States of America and the European Union, a definition containing the element of opprobrium is most appropriate: The *Global Terror Index* defines terrorism as the “threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation”⁵³⁴. Counterterrorism comprises all measures taken by governments and organizations to combat terrorism. These measures differ from country to country, because countries

⁵³¹ J. Bowyer Bell, *A Time of Terror: How Democratic Societies Respond to Revolutionary Violence* (New York: Basic Book, 1978); Alex Schmid, “Terrorism – The Definitional Problem”, *Case Western Reserve Journal of International Law* 36 (2004): 396. Accessed August 24, 2020, <https://scholarlycommons.law.case.edu/jil/vol36/iss2/8>.

⁵³² Schmid, “Terrorism – The Definitional Problem”, 396.

⁵³³ *Ibid.*, 405–407.

⁵³⁴ *Global Terrorism Index 2019 – Measuring the Impact of Terrorism*, Institute for Economics & Peace: 6. Accessed August 24, 2020, <https://www.economicsandpeace.org/wp-content/uploads/2020/08/GTI-2019web.pdf>.

face different types and degrees in terrorist threats and because they interpret these threats differently depending on their history and previous experiences with terrorist groups.

US and EU Counterterrorism After 9/11: Terrorism as War and Terrorism as Crime

The 9/11 attacks were unprecedented in their scale and nature and were quickly branded as a new form of terrorism that required new counterterrorism measures.

US counterterrorism

Following two major terrorist attacks in the 1990s, the Clinton administration identified terrorism as a priority and threat to national security and developed a counterterrorism strategy based on four policies: economic isolation, multilateral cooperation, increased resource allocation, and retaliation. Military strikes were conducted, but only reluctantly; the emphasis was on law enforcement⁵³⁵. This changed after the terrorist attacks of 9/11 in 2001.

The Bush administration had to face a lot of pressure and criticism for not having taken terrorism seriously enough and for having been unable to prevent the attacks. Its response to the attacks, announced before Congress, President George W. Bush proclaimed a long-term fight against terrorism and their supporters, referred to as the “Global War on Terror” (GWOT). He insisted that “[o]ur war on terror begins with al-Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped and defeated.”⁵³⁶. Instead of relying on ex-

⁵³⁵ Thomas J. Badey, “US counter-terrorism: Change in approach, continuity in policy”, *Contemporary Security Policy* 27, no. 2 (2006): 308–309.

⁵³⁶ Whitehouse Archives, “Address to a joint session of the 107th Congress”, by President George W. Bush, September 20, 2001, in *Selected Speeches of George W. Bush 2001–2008*: 68. Accessed August 24, 2020, https://georgewbush-whitehouse.archives.gov/infocus/bushrecord/documents/Selected_Speeches_George_W_Bush.pdf.

isting law enforcement policies and instruments, the Bush administration adopted a unilateral and military approach and assigned the lead in its counterterrorism efforts to the Department of Defense⁵³⁷. Condoleezza Rice explained the difference between the Clinton and the Bush administrations by declaring that President Clinton had called for bringing the terrorists from Afghanistan to the United States for trial, while President Bush prefers to prepare for military action in Afghanistan itself⁵³⁸. However, it is important to acknowledge that the US approach is not purely military; existing policies developed under the Clinton administration, for example economic isolation of terrorism sponsoring states, were maintained⁵³⁹.

Bush's choice in labeling the US response to terrorism a "Global War on Terror" was an unfortunate choice of vocabulary that has had long term political and legal implications. In a lecture given only a few weeks after the attacks, Oxford Professor Michael Howard referred to Bush's announcement as "a very natural but terrible and irrevocable error"⁵⁴⁰. The use of the term "war" in this context certainly makes a strong impression and emphasizes that the US government rejects any kind of "acquiescence or compromise"⁵⁴¹, but it has a couple of drawbacks: Firstly, a declaration of war is reciprocal and it gives terrorists a status and legitimacy that is normally reserved for states. Thus, the declaration of war raised Bin Laden's status as a warlord and as the one man, who challenged the most powerful nation in the world. Secondly, the state of war gives a free way to violence and puts at risk civilians' rights on the attacked territory as well as human rights in general. This is especially true for the specific rights foreseen by international law for fighters, for example in case of capture and detention. In comparison to a criminal, whose detention is punitive,

⁵³⁷ Badey, "US counter-terrorism", 308–309; Alberto Costi, "Complementary Approaches? A Brief Comparison of EU and United States Counter-Terrorism Strategies since 2001", *Victoria University of Wellington Legal Research Papers* 22 (2019): 178. Accessed August 24, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3074136.

⁵³⁸ *Ibid.*, 309.

⁵³⁹ *Ibid.*, 321.

⁵⁴⁰ Michael Howard, "What's in a name? How to fight terrorism", *Foreign Affairs* (January/February 2002): 8.

⁵⁴¹ Gilles Andréani, "The 'War on terror': Good Cause, Wrong Concept", *Survival* 46, no. 4 (2004): 31.

the detention of a fighter mainly prevents him from joining an ongoing war. Thirdly, the use of the term “war” creates an atmosphere of fear and belligerence, a “war psychosis”⁵⁴² that calls for immediate military actions expecting to result in the complete destruction of a clearly identified enemy. Suggestions that there are other options are dismissed as appeasement and concerns regarding the impact of war on non-state actors and the limits of armed force are not taken into consideration anymore. Besides, it exaggerates the threat of terrorism in the US compared to other security threats⁵⁴³. Ultimately, by referring to terrorist not only as unlawful, criminal actors, but as evil, the President actually leaves the sphere of international law and politics to enter the ground of moral judgement. This “evilization” of the enemy de-politicized the discourse about the War on Terror and gave it an almost religious glint⁵⁴⁴. Consequently, many Muslims in the Middle East and around the world considered the war on terror not only a war against Al-Qaeda, but a war against Islam and Muslims in general, despite the fact that Osama Bin Laden and his supporters are in no way representative for Muslims around the world⁵⁴⁵.

Apart from the drawbacks listed above, labeling the fight against terrorism a “war” simply is a misnomer⁵⁴⁶: President Bush admitted himself in 2004 that naming the 9/11 response a “Global War on Terror” was inappropriate. It should rather be called “the struggle against ideological extremists who do not believe in free societies and who happen to use terror as a weapon to try to shake the conscience of the free world.”⁵⁴⁷.

⁵⁴² Howard, “What’s in the name?”, 9.

⁵⁴³ Howard, “What’s in the name?”, 9; John Mueller, “Is There Still a Terrorist Threat?: The Myth of the Omnipresent Enemy”, *Foreign Affairs* (September/October 2006). Accessed August 24, 2020, <https://www.foreignaffairs.com/articles/2006-09-01/there-still-terrorist-threat-myth-omnipresent-enemy>.

⁵⁴⁴ Pamir H. Sahill, “The U.S. War on Terror Discourse”, *Insight Turkey. A New Scramble for Africa? The Role of Great and Emerging Powers*, 21:1 (2019), 190.

⁵⁴⁵ Costi, “Complementary Approaches?”, 180.

⁵⁴⁶ Andréani, “The ‘War on terror’”, 49; Frank Furedi, “Lost for Words”, *The Guardian*, January 17, 2008. Accessed August 24, 2020, <https://www.theguardian.com/commentisfree/2008/jan/17/lostfor-words>; Hendrik Hertzberg, “War and Words”, *The New Yorker*, February 6, 2006. Accessed August 24, 2020, <https://www.newyorker.com/magazine/2006/02/13/war-and-words>.

⁵⁴⁷ Ibid.

The only rightfully called war in the aftermath of 9/11 was the invasion of Afghanistan and the overthrow of the Taliban regime. It was led by the US, sanctioned by the United Nations Security Council, and received considerable offers of support from other states since the attack against the World Trade Centre was not only an attack on the United States of America, but on Western states in general, on their lifestyle and their values. Therefore, the attacks opened an opportunity window for the creation of an international counterterrorism alliance. However, by introducing the concept of preventive war to the war on terror, the US extended the situations under which they can go to war. While the Bush administration managed successfully to sell the invasion of Iraq to the American public as a second phase of the GWOT, it met a lot of opposition in Europe, among heads of government and diplomats as well as in civil society⁵⁴⁸. The invasion of Iraq split the US and EU, undermined the foundation of the international counterterrorism alliance, and led to divisions within Europe, because France and Germany were opposed to the invasion of Iraq, while Poland, Spain, and the United Kingdom were willing to support the US⁵⁴⁹.

The US approach to counterterrorism aimed at preventing potential future attacks⁵⁵⁰ and preferred short-term solutions against long-term progress. Bruce Hoffman insists that this is “not a matter of debate but rather was the conclusion of the declassified key judgments of the seminal April 2006 National Intelligence Estimate (NIE)”⁵⁵¹. Thus, the US approach was not successful in the long run, especially as the invasion and occupation of Iraq as well as the unlawful detention and torture of suspected terrorists allegedly increased the number of recruits of terrorist organizations such as ISIS and considerably damaged the US’ status and prestige internationally⁵⁵².

⁵⁴⁸ Andréani, “The ‘War on terror’”, 32–34; Alexander MacKenzie, “The European Union’s Increasing Role in Foreign Policy Counterterrorism”, *Journal of Contemporary European Research* 6, no. 2 (2010): 154. Accessed August 24, 2020, <http://www.jcer.net/ojs/index.php/jcer/article/view/269/214>.

⁵⁴⁹ Ibid.

⁵⁵⁰ Costi, “Complementary Approaches?”, 179.

⁵⁵¹ Bruce Hoffman, “A Counterterrorism Strategy for the Obama Administration”, *Terrorism and Political Violence* 21, no. 3 (2009): 360.

⁵⁵² Costi, “Complementary Approaches?”, 179; MacKenzie, “The European Union’s Increasing Role in Foreign Policy Counterterrorism”, 154; Muhammad Iqbal Roy, “The Global Counter-Terrorism

The Obama administration avoided referring to the Bush doctrine of “Global War on terror”. It also strived to build coalitions and to gain international support for its fight against terrorism. However, unilateral action still constituted as an option and the number of drones strikes increased under the Obama administration and were legitimized on the basis of the law of armed conflict. Thus, the Obama administration may have restrained itself from using the term “war”⁵⁵³, but its strategies in the fight against terrorism remained similar to the ones in use under the Bush administration⁵⁵⁴.

EU counterterrorism

Before 9/11, the member states of the European Union had to deal with terrorist attacks within their borders committed by domestic terrorist groups. These experiences shaped the approach of EU member states to terrorism as a matter of national security and their perception of terrorist acts as “criminal offenses to be tackled and contained”⁵⁵⁵, while the US aims to defeat terrorism for good and uses this aim to legitimize drone strikes, targeted killings, and detention of alleged combatants⁵⁵⁶.

This difference in approaches chosen by the US and the EU are due to a different perception of the threat and different governance arrangements⁵⁵⁷. The US does not have to deal with the same difficulties as the EU as it is able to “marshal its power at home”⁵⁵⁸. The EU is not a federal state and its counterterrorism measures are a matter of national security policies, even if the member states coordinate at the EU level. Besides, the US and the EU had different understandings of Al-Qaeda’s goal and there-

Strategies”, *Journal of Politics and International Studies* 5, no. 1 (2019): 26. Accessed August 24, 2020, http://pu.edu.pk/images/journal/politicsAndInternational/PDF/3_v5_1_2019.pdf.

⁵⁵³ MacKenzie, “The European Union’s Increasing Role in Foreign Policy Counterterrorism”, 154.

⁵⁵⁴ Costi, “Complementary Approaches?”, 179.

⁵⁵⁵ Costi, “Complementary Approaches?”, 178; Jeremy Shapiro, “Where You Stand Depends on Where You Get Hit: US and European Counterterrorism Strategies”, Security Studies Seminar, November 9, 2005, Brookings Institution. Accessed August 24, 2020, http://web.mit.edu/SSP/seminars/wed_archives05fall/shapiro.htm.

⁵⁵⁶ *Ibid.*, 175.

⁵⁵⁷ *Ibid.*, 167.

⁵⁵⁸ *Ibid.*, 178.

fore different interpretations of the threat they faced. The US considered Al-Qaeda to be at war against the West and its values, but from a European perspective, influenced by the tradition of Just War theory, wars can only be thought between states and should be governed by international law. An act of terrorism is thus not an act of war, but a criminal act and should be treated as such⁵⁵⁹.

Faithful to their approach of terrorism-as-crime, the first reaction of the EU to the 9/11 attacks was to toughen its criminal law instruments and to focus on threats within its borders⁵⁶⁰. EU leaders rapidly pushed for more integration in this area. The Council of the European Union adopted the Plan of Action to Combat Terrorism in September 2001, condemning the 9/11 attacks and acknowledging the common terrorist threat⁵⁶¹. In its 2002 Framework Decision on Terrorism, the EU provided its first common definition of terrorism and aims at aligning the Member States' positions on counterterrorism⁵⁶². The Council adopted in December 2003 a document entitled "A European Security Strategy – A Secure Europe in a Better World"⁵⁶³, containing a list of threats, which was headed by terrorism and called for a coordinated policy. After the attacks in Madrid in 2004 and London in 2006, the priority of counter-terrorism increased further and lead to an even deeper integration. The Declaration on Combating Terrorism and appointment of EU Counterterrorism Coordinator

⁵⁵⁹ Ibid., 173.

⁵⁶⁰ Ibid., 173–181.

⁵⁶¹ Council of the European Union, *Conclusions and plan of action of the extraordinary European Council meeting on 21 September 2001*, SN 140/01, September 21, 2001. Accessed August 24, 2020, <https://www.consilium.europa.eu/media/20972/140en.pdf>.

⁵⁶² Christine Andreeva, "EU Counter-terrorism Policy after 2015", *Institute of International & European Affairs (IIEA)*, (2019): 200. Accessed August 24, 2020, <https://www.iiea.com/wp-content/uploads/2019/06/Christine-Andreeva.pdf>; Mai'a K. Davis Cross, "Counter-terrorism in the EU's external relations", *Journal of European Integration* 39:5 (2017), 611; Javier Argomaniz, Oldrich Bureš and Christian Kaunert, "A Decade of EU Counter-Terrorism and Intelligence: A Critical Assessment", *Intelligence and National Security* 30:2–3 (2015): 191–206; Jörg Monar, "The EU as an International Counter-terrorism Actor : Progress and Constraints", *Intelligence and National Security* 30, no. 2–3 (2015): 333–356.

⁵⁶³ Council of the European Union, *A European Security Strategy – A Secure Europe in a Better World*, European Communities, 2009. Accessed August 24, 2020, <https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf>.

in March 2004⁵⁶⁴ increased cooperation between member states in the fields of security, cross-border crime, and terrorism. In 2005, the Council adopted the EU Counter-Terrorism Strategy based on four pillars: prevent, protect, pursue, and respond⁵⁶⁵. The EU Strategy for Combating Radicalization and Recruitment⁵⁶⁶ adopted in November 2005 recognized for the first time explicitly the issue of radicalization. The last substantial measure was the Revision of the Framework Decision on Terrorism in November 2008⁵⁶⁷. "Legislation adopted between 2001 and 2008 was deemed satisfactory as a legal framework for the initial stages of EU counter-terrorism policy."⁵⁶⁸

The first EU Counterterrorism Coordinator, Gijs de Vries, even considered the fight against terrorism as changing "the role and functioning of the European Union", arguing that the later adopts an "increasingly operational role"⁵⁶⁹. The most important innovation was the introduction of a new operational instrument, the European Arrest Warrant (EAW)⁵⁷⁰ and Europol, the EU Agency for Law Enforcement Cooperation, whose mandate was extended after 9/11, is at the heart of internal measures and clearly treats terrorism as a crime⁵⁷¹.

⁵⁶⁴ Council of the European Union, *Declaration on Combating Terrorism*, March 25, 2004. Accessed August 24, 2020, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/79637.pdf.

⁵⁶⁵ Council of the European Union, *Counter-terrorism strategy*, November 30, 2005. Accessed August 24, 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3AI33275>.

⁵⁶⁶ Council of the European Union, *The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism*, November 24, 2005. Accessed August 24, 2020, <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014781%202005%20REV%201>.

⁵⁶⁷ Council of the European Union, *Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism*, November 28, 2008. Accessed August 24, 2020, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32008F0919>; Andreeva, "EU Counter-terrorism Policy after 2015", 200.

⁵⁶⁸ Andreeva, "EU Counter-terrorism Policy after 2015", 199.

⁵⁶⁹ Oldrich Bureš, "EU Counterterrorism Policy: A Paper Tiger?", *e-International Relations*, August 22, 2013. Accessed August 24, 2020, <https://www.e-ir.info/2013/08/22/eu-counterterrorism-policy-a-paper-tiger/>.

⁵⁷⁰ Cross, "Counter-terrorism in the EU's external relations", 611; Argomaniz, Bureš, Kaunert, "A Decade of EU Counter-Terrorism and Intelligence", 191–206; Monar, "The EU as an International Counter-terrorism Actor", 333–356.

⁵⁷¹ Cross, "Counter-terrorism in the EU's external relations", 613.

A Shift in EU counter-terrorism policy: from internal threat to a matter of foreign policy

The series of attacks in Paris in 2015 were the deadliest since the Madrid metro bombing in 2004 and resulted in a wave of solidarity all over Europe and beyond, which created a favorable climate for policy advances and pushes. Besides, counterterrorism measures gained in support by public opinion: Eurobarometer research shows that terrorism has been among the main concerns for EU citizens since 2015⁵⁷².

After the attack on the satirical magazine “Charlie Hebdo” in January 2015, French President François Hollande promised a strong reaction and announced that “the Republic will be inflexible, implacable”⁵⁷³. When the “Charlie Hebdo” attacks in January were followed by attacks on several locations in Paris in November 2015, among them the “Stade de France” and the club “Bataclan”, a state of emergency was declared in France and the President announced that “France is at war”⁵⁷⁴ and that it will defend its values and “eradicate terrorism”⁵⁷⁵.

This unusually martial rhetoric, referring to the notion of “war”, the eradication of terrorism, the waging a good war, and the evilization of the enemy, bears a strong resemblance to the speeches of President George W. Bush after 9/11 and his “Global War on Terror”. Hollande’s Minister of Defense, Jean-Yves Le Drian, had already invoked the notion of a “war against terrorism” in January 2013, when referring to the French military intervention in Mali, revealing already the beginning of a turning

⁵⁷² Andreeva, “EU Counter-terrorism Policy after 2015”, 201.

⁵⁷³ Embassy of France in Washington, *Press conference given by M. François Hollande, President of the Republic* (excerpts), Paris, February 5, 2015, published on February 9, 2015. Accessed August 24, 2020, <https://fr.franceintheus.org/spip.php?article6498>.

⁵⁷⁴ Permanent Mission of France to the United Nations in New York, *François Hollande’s Speech Before a Joint Session of Parliament*, November 16, 2015. Accessed August 24, 2020, <https://onu.del-egfrance.org/Francois-Hollande-s-Speech-Before-a-Joint-Session-of-Parliament>.

⁵⁷⁵ Permanent mission of France to the United Nations in New York, *François Hollande’s Speech Before a Joint Session of Parliament*, November 16, 2015.

point in the French approach of the fight against terrorism⁵⁷⁶. Discourse analysis of Hollande's speeches in 2015 revealed "a carefully constructed public communication strategy"⁵⁷⁷, instilling fear by using a "language of exception"⁵⁷⁸ and conjuring a climate similar to the aforementioned "war psychosis". Another indicator for the shift in approach to counterterrorism is the fact that Spain and the United Kingdom were both hit before France by major terrorist attacks in 2004, respectively 2005, but they considered direct military actions against Al-Qaeda at that moment as either unjustifiable or counterproductive⁵⁷⁹. Meanwhile, their positions have changed: "the UK, Germany, Belgium, the Netherlands, Denmark, Italy, Spain, and Poland have all been directly involved in conducting or assisting military action against jihadist groups in the regions surrounding Europe."⁵⁸⁰.

Already prepared by the revision of the EU Strategy for Combating Radicalisation and Recruitment to Terrorism in 2014⁵⁸¹, the attacks in 2015 clearly marked a shift in tone and approach in EU counterterrorism – a shift that was further enhanced by the terrorist attacks in 2016, namely the bombing of the Brussels Airport, the explosion of Maalbrek metro station, and the cargo truck driven into crowds in Nice on 14th of July. They opened a window of opportunity for policy-makers and "[t]hese 15 months generated more efforts on counter-terrorism at EU level than the preceding

⁵⁷⁶ Alice Pannier and Olivier Schmitt, "To fight another day: France between the fight against terrorism and future warfare", *International Affairs* 95, no. 4 (2019): 905.

⁵⁷⁷ Ariane Bogain, "Security in the name of human rights: the discursive legitimization strategies of the war on terror in France", *Critical Studies on Terrorism* 10, no. 3 (2017): 477.

⁵⁷⁸ Bogain, "Security in the name of human rights", 484; Grégory Chauzal, Ko Colijn, Bibi van Ginckel, Christophe Paulussen and Sofia Zavagli, "Paris: 11/13/15 – Analysis and Policy Options", Policy Brief, *Clingendael Netherlands Institute for International Relations*, November 20, 2015. Accessed August 24, 2020, https://www.clingendael.org/sites/default/files/2017-06/Policy_Brief_Clingendael_IC-CT-Paris111315Analysis_and_Policy_Options_November%202015_final.pdf; Giorgio Agamben, *State of Exception*, Chicago University Press (2005).

⁵⁷⁹ Anthony Dworkin, "Europe's New Counter-Terror Wars", Policy Brief, *European Council on Foreign Relations*, October 2016, 3. Accessed August 24, 2020, https://www.ecfr.eu/page/-/ECFR192_-EUROPES_NEW_COUNTER-TERROR_WARS_FINAL.pdf.

⁵⁸⁰ Dworkin, "Europe's New Counter-Terror Wars", 2.

⁵⁸¹ Council of the European Union, *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, May 19, 2014. Accessed August 24, 2020, <https://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf>.

15 years.”⁵⁸². Immediately after the attack on Charlie Hebdo in January 2015, three Council Conclusions were adopted soon after: the Justice and Home Affairs (JAI) Council Conclusions of 30 January 2015, the Foreign Affairs Council (FAC) Conclusions of 9 February 2015, and the Informal Heads of State Summit Conclusions of 12 February 2015⁵⁸³. While having been considered a mainly internal issue, the FAC Conclusions of 9 February 2015 acknowledged for the first time the external dimension of the terrorist threat and established the basis for strengthening external action on counterterrorism⁵⁸⁴. The 2005 EU Counter-Terrorism Strategy already prepared the ground and the Terrorism Action Plan, adopted in 2016, emphasized the external actorness of the EU⁵⁸⁵. Thus, the EU counterterrorism took gradually a much more external dimension, governed by the European External Action Service (EEAS) that deals with the EU’s foreign policy⁵⁸⁶.

In a joint contribution to the European Political Strategy Centre, **Federica Mogherini** and **Sir Julian King** acknowledged in 2017 the link between internal and external security and emphasized that the EU’s engagement outside its territory is essential for the safety of EU citizens and complementary to internal counterterrorism measures. They both point out that the EU’s cooperation with international partners has grown in the past two years⁵⁸⁷.

US-EU convergence in counterterrorism?

While the fight against terrorism initially divided the EU and the US, they cooperated more closely in the past years. However, as their relationship is an asymmetrical one, the EU tended to become a norm-taker instead

⁵⁸² Andreeva, “EU Counter-terrorism Policy after 2015”, 198–199.

⁵⁸³ *Ibid.*, 202–203.

⁵⁸⁴ *Ibid.*, 202–203.

⁵⁸⁵ Argomaniz, Bureš, Kaunert, “A Decade of EU Counter-Terrorism and Intelligence”, 191–206.

⁵⁸⁶ Cross, “Counter-terrorism in the EU’s external relations”, 609–613.

⁵⁸⁷ Federica Mogherini and Sir Julian King. “Navigating the internal-external security nexus”, *EU Security and Defence in a Volatile World*, European Political Strategy Centre (2017). Accessed August 24, 2020, <https://medium.com/eu-security-and-defence-in-a-volatile-world/navigating-the-internal-external-security-nexus-1dc2ed213f380>.

of being a norm-maker, especially under political pressure following major terrorist attacks. Hence, during negotiations, it had to adopt US security norms, which did not coincide with European principles in matters of human rights and data protection⁵⁸⁸. This was the case for the Passenger Name Record (PNR) agreement, which the European Parliament initially vetoed because of concerns regarding data protection and human rights. The French President Hollande pressured for the PNR to be adopted, arguing that it is vital for tracking suspected terrorists⁵⁸⁹, and the Brussels attacks in March 2016 further enhanced political pressure on the European Parliament resulting in the PNR Package being suddenly adopted within weeks, on the 21st of April 2016⁵⁹⁰. Moreover, EU member states also have accepted to collaborate with the CIA regarding the detention of suspected terrorists and thus engaged in or at least tolerated human rights violations. EU member states also risk following the US in setting dangerously legal precedents for their military actions abroad⁵⁹¹.

The EU is increasingly embracing the external dimension of counterterrorism and cooperates with the US in this area, despite its reluctance to support the US war approach after 9/11. The transatlantic divide, or transatlantic crisis, caused by the invasion of Iraq was a low-point in US-EU relations and made many experts worry about the future of the West. Thus, cooperation between the US and the EU is welcome and necessary for a successful fight against terrorism. The US and the EU have to pool their resources and exchange intelligence to prevent future terrorist attacks and radicalization of its youth.

However, the EU should be careful not to embrace a counterterrorism policy based mainly on military strikes. As mentioned earlier, the US approach

⁵⁸⁸ MacKenzie, "The European Union's Increasing Role in Foreign Policy Counterterrorism", 158; Javier Argomaniz, "When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms", *Journal of European Integration* 31, no. 1 (January 2009): 119–136.

⁵⁸⁹ Bogain, "Security in the name of human rights", 488.

⁵⁹⁰ Andreeva, "EU Counter-terrorism Policy after 2015", 205; Cross, "Counter-terrorism in the EU's external relations".

⁵⁹¹ Dworkin, "Europe's New Counter-Terror Wars", 2.

and the related human rights violations led to a rise in terrorist recruits⁵⁹² and the French military strikes in Syria in 2015 led to “the first high-casualty attacks directly organised by ISIS in Europe”⁵⁹³, i.e. the Paris attacks in November 2015 and the Brussels bombings in March 2016. Thus, a military approach can be counterproductive. It might even intensify existing tensions and cause more material damage and casualties among civilians than another approach might have done. Moreover, it does not target the root causes for terrorist attacks, which often lie in a lack of social inclusion and intercultural dialogue. Some European officials have not forgotten the dangers that lie in adopting a war paradigm. Despite the show of solidarity with France after the Paris attacks and the support for its military actions, European officials were uncomfortable with the martial rhetoric adopted by President Hollande⁵⁹⁴. German Vice Chancellor Sigmar Gabriel declared that “talking about war would constitute a first success for the Islamic State”, Italian Prime Minister Matteo Renzi stated that “Italy wasn’t at war.”, and Prime Minister Mariano Rajoy of Spain explicitly rejected any reference to war in this context⁵⁹⁵. Accordingly, the Clingendael Netherlands Institute for International Relations warns that “[l]anguage matters and such statements [of President Hollande] are reminiscent of US President Bush’s post-9/11 counterproductive approach, and could potentially open the door to disproportional responses, including violations of human rights and the principles of the rule of law. These statements also feed into the terrorists’ own rhetoric and intent to draw France and others into the war paradigm. These dreadful terrorist attacks should be dealt with, in a sober manner, via, amongst other things, regular criminal law.”⁵⁹⁶. As mentioned before, the EU has already become less reluctant to put human rights concerns aside in order to push the adoption of contested counterterrorism measures.

⁵⁹² Costi, “Complementary Approaches?”, 179; MacKenzie, “The European Union’s Increasing Role in Foreign Policy Counterterrorism”, 154; Roy, “The Global Counter-Terrorism Strategies”, 26.

⁵⁹³ Dworkin, “Europe’s New Counter-Terror Wars”, 5.

⁵⁹⁴ Dworkin, “Europe’s New Counter-Terror Wars”, 5.

⁵⁹⁵ Simond de Galbert. “After the Paris Attacks, France Turns to Europe in its Time of Need”, Commentary, *Center for Strategic and International Studies* (2015). Accessed August 24, 2020, www.csis.org/analysis/after-paris-attacks-france-turns-europe-its-time-need.

⁵⁹⁶ Chauzal, Colijn, van Ginkel, Paulussen and Zavagli, “Paris: 11/13/15”, 2.

Nevertheless, France is not the only EU member state that has meanwhile engaged in or assists military operations against terrorists outside of its territory, even if these operations are not the only pillar of EU counterterrorism. “[T]hese operations mark a departure from the previous practice of EU member states, and European governments appear to have paid little attention to the risks they entail.”⁵⁹⁷ Military actions might not help to achieve the goal of fighting terrorism and guarantee safety of EU citizens. On the contrary, after drone strikes by the UK in August 2015 and the extension of the French military campaign against terrorists in Syria in September 2015, Europe got hit by the first “high-casualty attacks directly organised by ISIS in Europe”⁵⁹⁸, namely the Paris attacks of November 2015, the Brussels airport bombing and the explosion in Maelbeek metro station.

Considering the above, US and EU practices in using military forces have come closer together: While some EU member states have decided to fight terrorism not only with law enforcement instruments, but also by conducting military operations, the US included a greater counter-insurgent element into their military operations against terrorists⁵⁹⁹. According to Dworkin, “[t]here has been an unnoticed convergence in the military practice of European countries and the US.”⁶⁰⁰

However, convergence does not mean duplication and duplication would not be possible as the US and the EU do not share the same institutional and operational set-up. The primary responsibility in counterterrorism policy still lies with the EU member states, even if the EU role in this policy area has increased in the past years. Besides, military strikes are not the major part of EU counterterrorism efforts. Thus, there certainly is a convergence of US and EU counterterrorism, at least in the military aspects of it, but differences remain and always will. Even if counterterrorism is growing into an important common policy area, it is unlikely that member states will ever hand over responsibility for their citizens’ safety. Counterterrorism

⁵⁹⁷ Dworkin, “Europe’s New Counter-Terror Wars”, 1–2.

⁵⁹⁸ *Ibid.*, 5.

⁵⁹⁹ *Ibid.*, 14.

⁶⁰⁰ *Ibid.*, 1.

continues to be a hybrid policy with shared competence between US and the EU, but it has clarified its mandates, introduced new instruments and defined their utilization and there is a high common threat perception within the EU⁶⁰¹.

Conclusion

War on terror has not made the world any safer. On the contrary, it was even counterproductive. Hence, it should not be taken as a role model to follow, not even for rhetorical purposes. As mentioned in this paper, words matter, especially in the area of international politics and terrorism, and political leaders should be aware of the implication of their choice of words. While the transatlantic divide in the aftermath of 9/11 was deplorable, it might have given the EU member states the opportunity to develop a common counterterrorism policy, which they would probably not have done, if they had simply followed the Bush administration's lead.

If it is true that law enforcement instruments are not enough to fight international terrorism, states should restrain from unnecessary or ineffective military operations. Military strikes should never be the first choice to react to terrorist attacks as the costs, risks and civil casualties might be much higher than estimated beforehand. While cooperation between the US and the EU is welcome, experts, policy makers and citizens should keep an eye on the convergence of their counterterrorism policies. Mistakes of the past should be avoided and blind obedience cannot be a condition for cooperation and mutual support. The US and the EU share a history and values and should be allies in the fight against terrorism. However, they are also different in some respects and operate out of a different institutional setting. Their differences in policy approaches should be complementing, not dividing each other.

I agree with Dworkin, who urges EU member states to show more consideration and restraint in military operations and to "help reinforce an

⁶⁰¹ Andreeva, "EU Counter-terrorism Policy after 2015", 210.

international order in line with the EU's interests and values"⁶⁰². The same applies to the US, whose international status suffered from the "Global War on Terror". With Aronofsky's words, "The U.S. war on terror has created many casualties. Perhaps the greatest casualty of all is a loss of the core rule of law focus, which differentiated the U.S. from so many other countries on the global stage decades before this war began. In order to win it, the U.S. must regain its leadership in not only advocating, but practicing rule of law principles predicated on respect for, and protecting, basic individual rights."⁶⁰³.

⁶⁰² Dworkin, "Europe's New Counter-Terror Wars", 1–2.

⁶⁰³ David Aronofsky. "The War on Terror: Where We Have Been, Are, and Should Be Going", *Denver Journal of International Law & Policy* 40, no. 1, April 2020, 105.

Article 5 and the Challenges of Cyber Defense

Theo WARNER

Abstract: As cyberspace expands to encompass all aspects of life, so too do the vulnerabilities of critical infrastructure and information expand. The North Atlantic Treaty Organization (NATO) historically has been a force for collective defense and has not shied away from meeting developing cyberthreats from state and non-state entities alike. The primary objective of this short paper is to highlight the unique nature of cyber defense and countering cyberattacks, particularly in the context of NATO's Article 5. I will briefly discuss the language of Article 5, as well as a few of the major challenges that could arise if the article (or any sort of international legal action) were invoked in response to some serious cyberattack, particularly attribution and proportionality, using the infamous 2007 cyberattack against Estonia as a brief case study.

Keywords: Cybersecurity, Cyber Defense, NATO, Article 5, Collective defense, Collective security, Attribution, Proportionality

Introduction

In the late 1980s and early 1990s, the communist system of the Eastern Bloc and Soviet Union disintegrated. The Berlin Wall was toppled in 1989, the Warsaw Pact was dissolved in 1991, and NATO quite suddenly found itself navigating a post-Soviet Europe⁶⁰⁴. As the 1990 NATO Update

⁶⁰⁴ Hella Pick, "NATO seeks a new role", *The Guardian*, May 18, 1990, <https://www.newspapers.com/image/260321413/>.

remarked, “the breathless pace of change does not stop.”⁶⁰⁵ Though born in the fledgling years of the Cold War, NATO did not perish with the Soviet Union. In the 21st century, NATO’s strategy has shifted to meet new threats, including the rising danger posed by coordinated state-sponsored and non-state cyberattacks⁶⁰⁶.

Though coordinated cyberattacks were already causing growing concern in the late nineties, cyber threats shot to the forefront of NATO’s security worries in the wake of the massive cyberattack against Estonia in 2007. Since then, NATO has expanded its cyber defense research and capabilities, establishing the Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in 2008 and sponsoring the publishing of the first edition of the Tallinn Manual on the International Law Applicable to Cyber Warfare in 2013. In August 2019, NATO Secretary General Jens Stoltenberg warned that “a serious cyberattack could trigger Article 5 of our founding treaty.”⁶⁰⁷

Article 5 is the cornerstone of the collective security agreement codified in the 1949 Washington Treaty that states “an armed attack against one or more of [NATO members] in Europe or North America shall be considered an attack against them all.”⁶⁰⁸ The drafters of the treaty did not likely anticipate the scale of interconnectedness brought on by global cyber networks in the 21st century. The world has gotten smaller and information systems, including private and public, rely on innovations in the cybersphere now more than ever before⁶⁰⁹.

⁶⁰⁵ “1990: Summary”, NATO Update, last modified August 23, 2001, accessed 11 August, 2020, <https://www.nato.int/docu/update/1990/summarye.htm>.

⁶⁰⁶ “Statement by the North Atlantic Council concerning malicious cyber activities”, NATO, last modified June 3, 2020, accessed August 11, 2020, https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en.

⁶⁰⁷ “NATO will defend itself”, NATO, last modified August 29, 2019, accessed August 11, 2020, https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en.

⁶⁰⁸ “The North Atlantic Treaty”, NATO, last modified April 10, 2019, Accessed August 11, 2020, https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

⁶⁰⁹ Sitara Noor, “Cyber (In) Security: A Challenge to Reckon With”, *Strategic Studies* 34, no. 2/3 (2014): 1–19, accessed August 12, 2020, doi:10.2307/48527537.

Article 5, buttressed by NATO's conventional defensive capabilities, has acted as a powerful deterrent against acts of aggression against member states⁶¹⁰. Though the Secretary General's warning was likely a type of "cyber-deterrence", it is nevertheless worth examining what a deployment of Article 5 under such conditions would look like.

Cyberspace has solidified itself as a crucial component of the "fifth domain." Just as land, sea, air, and space are domains through which war is waged, cyberspace exists as a growing part of the information operations domain⁶¹¹. In 1999, members of the Pentagon's Joint Task Force for Computer Network Defense warned that in the case of a cyber war critical infrastructure including air traffic control and financial systems could be "held hostage."⁶¹² More than twenty years later, cyberspace has permeated nearly all aspects of contemporary life, including commerce, finance, and military. This growing reliance on cyberspace increases the susceptibility of necessary aspects of society to attack. As former president of Estonia Toomas Hendrik Ilves points out, "the more modern and the more digitized you are, the more vulnerable you are."⁶¹³

In spite of rising global threats, NATO's relevance in the 21st century has come under growing criticism, particularly from political leadership within the United States⁶¹⁴. American President Donald Trump has frequently questioned the extent of the United States' financial commitment to

⁶¹⁰ Edgar Buckley and Ioan Mircea Pascu, "Article 5 and Strategic Reassurance", (Washington DC: The Atlantic Council, 2010), accessed August 14, 2020, www.jstor.org/stable/resrep03320.

⁶¹¹ Can Kasapoglu, "Cyber Security: Understanding the Fifth Domain", (Istanbul: Centre for Economics and Foreign Policy Studies, 2017), accessed August 11, 2020, www.jstor.org/stable/resrep14048.

⁶¹² David Abel, "Hackers kept allies on the defensive", *The Boston Globe*, June 20, 1999, accessed August 11, 2020, <https://www.newspapers.com/image/441818908>.

⁶¹³ Toomas Hendrik Ilves, "The Consequences of Cyber Attacks", *Journal of International Affairs* 70, no. 1 (2016): 175–81, accessed August 14, 2020, www.jstor.org/stable/90012601.

⁶¹⁴ Phil Stewart and Idrees Ali, "U.S. to withdraw about 12,000 troops from Germany but nearly half to stay in Europe", *Reuters*, July 29, 2020, accessed 11 August 2020, <https://www.reuters.com/article/us-usa-trump-germany-military/u-s-to-withdraw-about-12000-troops-from-germany-but-nearly-half-to-stay-in-europe-idUSKCN24U20L>.

the organization and has avoided explicitly endorsing Article 5⁶¹⁵. Though high profile voices in American political discourse have affirmed the U.S.'s commitment to Article 5, including James Mattis, Mike Pompeo, and Mike Pence, the lack of acknowledgement from the head of state has fomented anxiety among NATO member states^{616, 617}. French President Emmanuel Macron has lambasted American distancing from the organization, dubbing recent developments the "brain death of NATO"⁶¹⁸.

The growing danger posed by cyberthreats as well as the presently tepid relationship between the United States and NATO stress the importance of continued study into the challenges of mitigating future attacks. Though this article is limited in scope, I hope to expand on the logistical problems involved in responding to cyberattacks, particularly as it relates to Article 5 of the Washington Treaty.

Defining Terms: NATO and Cyberspace

NATO was established on 4 April 1949 with the signing of the Washington Treaty and has grown considerably since its inception. At its founding, NATO had 12 members. To date, 30 members are in NATO, with the most recent addition being North Macedonia in March 2020⁶¹⁹. NATO's founding treaty establishes the standard of collective defense binding the member states. This notion is enshrined in Article 5, which states in part:

⁶¹⁵ Rosie Gray, "Trump Declines to Affirm NATO's Article 5", *The Atlantic*, May 25, 2017, accessed August 14, 2020, <https://www.theatlantic.com/international/archive/2017/05/trump-declines-to-affirm-natos-article-5/528129/>.

⁶¹⁶ Gray, "Trump Declines".

⁶¹⁷ Dave Reynolds, "Hailing NATO, Pompeo urges alliance to counter new threats", Share America, November 21, 2019, accessed August 14, 2020, <https://share.america.gov/pompeo-hails-nato-urges-it-counter-new-threats/>.

⁶¹⁸ "Emmanuel Macron warns Europe: NATO is becoming brain-dead", *The Economist*, November 7, 2019, accessed August 11, 2020, <https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead>.

⁶¹⁹ "Member countries", NATO, last modified March 24, 2020, accessed August 14, 2020, https://www.nato.int/cps/en/natohq/topics_52044.htm.

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area⁶²⁰.

In NATO's 71-year history, Article 5 has only been invoked once in response to the September 11, 2001 terrorist attacks against the United States. A cyberattack large enough in scale to trigger Article 5 would be wholly unprecedented, thus attempting to predict the future or envision what such an event would look like would be exceedingly ambitious for a paper of this scope. Nevertheless, the language employed in Article 5 and the broader issues involving an international response to a cyberattack are worth examining.

Cyberspace is the environment through which digital information is sent, received, and stored. NATO recognizes cyberspace as a unique operational domain, including it with the conventional domains of air, land, and sea⁶²¹. This classification as an operational domain expands NATO's defense capabilities. As Gen. Larry D. Welch further writes, cyberspace is the domain "embedded in all domains."⁶²² Technological advancement in the conventional domains has become invariably bound with advancements in cyber capabilities.

Cyberspace is a vast domain that can be divided into more manageable subdomains. The Tallinn Manual stratifies cyberspace into three layers: the physical layer, the logical layer, and the social layer⁶²³. The physical layer

⁶²⁰ "The North Atlantic Treaty".

⁶²¹ "NATO will defend itself".

⁶²² Larry Welch, "Cyberspace – The Fifth Operational Domain", IDA, 2011, <https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace--the-fifth-operational-domain.ashx>.

⁶²³ Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed, (Cambridge: Cambridge University Press, 2017), 12, doi:10.1017/9781316822524.

refers to the tangible “network components”, including infrastructure like computers and servers, the logical layer is the series of connections that interlink the physical layer, including “applications, data and protocols”, and the social layer includes the interactions between people in cyberspace⁶²⁴. The proliferation of the internet has cultivated a physical, logical, and social infrastructure that is susceptible to cyberattacks.

A cyberattack is an assault on any of the aforementioned layers of cyberspace – physical, logical, or social. “Cyberattack” is an unavoidably catch-all term that ranges from nuisance phishing scams or distributed denial of service (DDoS) attacks to a damaging or even deadly assault on a power grid⁶²⁵. This wide range in severity contributes in part to the difficulty of establishing international legal standards and expectations for responding to cyberattacks.

NATO is no stranger to cyberattacks. The earliest targeted attacks against the organization took place in the late nineties. In the spring of 1999, in the midst of the NATO bombing of Yugoslavia during the Kosovo War, NATO’s computer systems in Brussels were bombarded with “thousands of e-mails and potent computer viruses” which briefly crippled the organizations cyber infrastructure⁶²⁶. In 2007 Estonia, which acquired NATO membership in 2004, experienced a series of coordinated cyberattacks linked to Russian operatives⁶²⁷. In 2014, in the midst of tensions over the Crimean crisis, NATO websites were hit by a series of DDoS attacks linked tentatively to pro-Russian “hacktivists.”⁶²⁸. Though these attacks range in severity, they all fall under the same umbrella.

⁶²⁴ Schmitt, *Tallinn Manual*.

⁶²⁵ Brian Barrett, “Security News This Week: An Unprecedented Cyberattack Hit US Power Utilities”, *Wired*, September 7, 2019, accessed August 14, 2020, <https://www.wired.com/story/power-grid-cyberattack-facebook-phone-numbers-security-news/>.

⁶²⁶ Abel, “Hackers”.

⁶²⁷ Alison Lawlor Russell, “Cyber Attacks on Estonia”, In *Cyber Blockades*, (Washington, DC: Georgetown University Press, 2014), 69–95, www.jstor.org/stable/j.ctt9qdsfj.9.

⁶²⁸ Adrian Croft and Peter Apps, “NATO websites hit in cyber attack linked to Crimea tension”, *Reuters*, March 15, 2014, accessed August 14, 2020, <https://www.reuters.com/article/us-ukraine-nato/nato-websites-hit-in-cyber-attack-linked-to-crimea-tension-idUSBREA2E0T320140316>.

Cyber defense is the action taken to prevent a cyberattack. At present, NATO has made clear that cyber defense is a core component of collective defense, however the early 2000s witnessed a relatively limited endeavor to preempt cyberthreats⁶²⁹. The 2002 Prague Summit Declaration, which included a lengthy pledge to counter terrorism and expand NATO's conventional forces, dedicated a one-line commitment to cyber defense: "[To] strengthen our capabilities to defend against cyberattacks."⁶³⁰ Since the now infamous 2007 cyberattacks in Estonia, NATO's cyber defense apparatus has expanded considerably. The organization has underscored not only its commitment to cyber defense, but to deterrence and countering "malicious cyber activities"⁶³¹. This commitment was pronounced by Secretary General Stoltenberg's statements cautioning that the collective security assured by Article 5 extended to "serious" cyberattacks.

Article 5 and Countering Cyberthreats

Article 5 embodies the "principle of collective defense"⁶³². The assurance that an attack on one is an attack on all acts as a force that binds members together, however this force is largely theoretical as the article has only been invoked once in the history of the alliance.

The language of Article 5 is purposefully flexible, requiring that events triggering its invocation be handled on a case-by-case basis. The article sponsors "such action as it deems necessary...to restore and maintain [security]" in response to an "armed attack"⁶³³. Of course, "such action as it deems necessary" is not a precise blueprint, and the restoration of "secu-

⁶²⁹ "Cyber defense", NATO, March 17, 2020, accessed August 14, 2020, https://www.nato.int/cps/en/natohq/topics_78170.htm.

⁶³⁰ "Prague Summit Declaration", NATO, May 6, 2014, accessed August 11, 2020, https://www.nato.int/cps/en/natohq/official_texts_19552.htm?text=Article%20%20provides%20that%20if%20to%20assist%20the%20Ally%20attacked.

⁶³¹ "Statement by the North Atlantic Council".

⁶³² "Collective defense – Article 5", NATO, last modified November 25, 2019, accessed August 17, 2020, https://www.nato.int/cps/en/natohq/topics_110496.htm#:~:text=Article%20%20provides%20that%20if%20to%20assist%20the%20Ally%20attacked.

⁶³³ "The North Atlantic Treaty".

ity” is not a precise goal. Though Article 5 specifies that an “armed attack” will trigger its invocation, it does not necessitate an armed response, only that all members of the organization respond in some measure. NATO has the ability to respond to an attack with the means it sees fit and has jurisdiction to determine when that response is adequate.

In the context of the Washington Treaty, NATO has indicated that a “serious” cyberattack is equivalent to an “armed attack.” This is evidenced by Secretary General Stoltenberg’s warning that NATO could invoke Article 5 in the event of a “serious” cyberattack as well as the 2018 Brussels Summit Declaration which declared that “Cyber defence is part of NATO’s core task of collective defence.”⁶³⁴ As mentioned before, the activities that amount to a cyberattack range vastly in severity. Determining which actions constitute a cyberattack in the eyes of international law, let alone a “serious” cyberattack, is of great importance when confronted with *jus ad bellum*.

The language equivocating “armed” attacks to cyberattacks was further parsed in the second edition of the Tallinn Manual. In wake of the 2007 cyberattacks in Estonia, the newly established NATO CCD COE spearheaded the publication of the Tallinn Manual on the International Law Applicable to Cyber Warfare, a study examining the limits of international law when it comes to cyberspace⁶³⁵. The initial study was published in April 2013 and the second edition followed shortly thereafter in 2017. The study devotes a chapter towards discussion of when a cyberattack constitutes a “use of force” (i.e. an “armed attack”) and establishes that “some cyber actions are undeniably not uses of force, uses of force need not involve a State’s direct use of armed force, and all armed attacks are uses of force.”⁶³⁶

With that framework established, the study delves into methods of assigning levels of severity to cyberattacks. Whether or not a cyberattack meets the “use of force threshold” is determined by factors including severity,

⁶³⁴ “Brussels Summit Declaration”, NATO, last modified August 30, 2018, accessed August 14, 2020, https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20.

⁶³⁵ Schmitt, *Tallinn Manual*.

⁶³⁶ Schmitt, *Tallinn Manual*, 333.

immediacy, and directness, to name a few⁶³⁷. The first factor, severity, is the “most significant”⁶³⁸. As they describe, severity lies on a spectrum ranging from inconvenience to physical harm. The former will “never” qualify as a use of force while the latter is invariably so⁶³⁹. Where an attack places on this scale of severity determines its categorization as “use of force”.

The study notes the ambiguity that can arise when characterizing a cyberattack as a use of force. They write: “a highly invasive operation that causes only inconvenience, such as temporary denial of service, is unlikely to be classified as a use of force. By contrast, some may categorise massive cyber operations that cripple an economy as a use of force...”⁶⁴⁰. In short, disagreements over what is and is not a cyberattack seem destined to occur, which only make the logistics of any serious consideration of Article 5 murkier.

Issues of territoriality and jurisdiction further complicate international legal processes in cyberspace. As defined earlier, cyberspace is a vast and nebulous environment. This is not as true for the physical layer; however, the logical and social layer are highly abstract in the context of territoriality. As Erin Anzelmo writes, “The internet exists in an immaterial dimension”⁶⁴¹. It does not abide by the conventional rules of geographic territoriality. This unique facet of cyberspace proves to be more of an issue for disputes in international court, however the territoriality question also bleeds into the issue of attribution⁶⁴².

The Washington Treaty makes some note of territoriality in Article 6, which serves to expand upon Article 5. It states that “an armed attack on one or

⁶³⁷ Ibid, 334.

⁶³⁸ Ibid.

⁶³⁹ Ibid.

⁶⁴⁰ Ibid, 337.

⁶⁴¹ Erin L. Anzelmo, “Cyberspace in International Law: Does the Internet Negate the Relevance of Territoriality in International Law?” *Studia Diplomatica* 58, no. 4 (2005), 155, <https://www.jstor.org/stable/44839534?seq=1>.

⁶⁴² Anzelmo, “Cyberspace in International Law”, 157–159. Anzelmo examines issues associated with proposed methods of determining jurisdiction that place emphasis on nationality and geography.

more of the Parties is deemed to include an armed attack: on the territory of any of the Parties in Europe or North America ...[or] on the forces, vessels, or aircraft of any of the Parties..."⁶⁴³. Cyber infrastructure (territory) is included by virtue of NATO's earlier guarantees that Article 5 applies to cyberattacks.

More than issues of treaty language, attribution and limited evidence present the most vexing roadblock when responding to cyberattacks. More often than not, attributing an attack's origin with certainty is all but beyond the realm of possibility⁶⁴⁴. The US ODNI optimistically dubs the process, "difficult but not impossible"⁶⁴⁵. The difficulty increases substantially, however, when attempting to trace the entity responsible for directing the attack⁶⁴⁶. Accurately identifying the actor responsible, especially if the attack was state-sponsored, is necessary before any counter-response can be crafted.

Attribution is the action of assigning blame. In cyberspace, this proves difficult for a myriad of reasons. For one, identifying an individual is entirely possible, but connecting that culpable individual's motivation to a state proves challenging. Benjamin Edwards et al. point out that "In a world where nonstate actors can readily acquire the ability to conduct cyberattacks, holding a government responsible, even for attacks originating within its borders, is not easy."⁶⁴⁷ They further describe issues associated with attribution, including the ease with which digital evidence can be "spoofed" and digital traces erased⁶⁴⁸.

⁶⁴³ "The North Atlantic Treaty".

⁶⁴⁴ Jan Dymet, "The Cyber Attribution Dilemma: 3 Barriers to Cyber Deterrence", Security Intelligence, December 28, 2018, accessed August 17, 2020, <https://securityintelligence.com/the-cyber-attribution-dilemma-3-barriers-to-cyber-deterrence/>.

⁶⁴⁵ US Office of the Director of National Intelligence, *A Guide to Cyber Attribution*, by the NIO and the National Intelligence Manager for Cyber, Washington, DC: ODNI, 2018, https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf (Accessed August 14, 2020).

⁶⁴⁶ US ODNI, *A Guide to Cyber Attribution*.

⁶⁴⁷ Benjamin Edwards et al. "'Strategic Aspects of Cyberattack, Attribution, and Blame", *Proceedings of the National Academy of Sciences of the United States of America* 114, no. 11 (2017): 2825, accessed August 17, 2020. doi:10.2307/26480254.

⁶⁴⁸ Edwards, "Strategic Aspects", 2825.

The issue of attribution played a significant role in the oft-cited 2007 cyber-attack against Estonia. In 2007, Estonia was miles ahead of the global curve in cyberspace. Described as a “leader in ... e-governance”, Estonia has relied on the internet for carrying out a wide range of social necessities and services⁶⁴⁹. In a 2016 interview with the *Journal of International Affairs*, former Estonian president Toomas Hendrik Ilves describes this integration of the internet and public services, commenting that “...Almost all of bank transactions and income tax returns have been done online since 2000, virtually all prescriptions are online, the land registry exists only digitally, and one third of votes in the last several elections were cast online.”⁶⁵⁰. As he later points out, however, Estonia’s reliance on the internet left it vulnerable to attack.

The inciting incident was the relocation of the Bronze Soldier of Tallinn, a Soviet-era war memorial erected in 1947⁶⁵¹. The statue had stood in a city park in Estonia’s capital, however early in 2007 the Estonian Parliament, in spite of threats from neighboring Russia, voted to move the monument in addition to adjacent war graves⁶⁵². Protests, and eventually riots, erupted, most notably from ethnic Russians living in Estonia who took issue with the statues relocation.

Shortly thereafter, Estonia suffered a series of cyberattacks unprecedented in their scale and coordination. A day after the statue was relocated, Estonian government sites were inundated with an abnormally large amount of traffic. The next day, the state’s mail server was spammed with thousands of emails, causing the Estonian Parliament’s server to crash. Media, banking and political websites were overwhelmed by DDoS attacks and an internet service provider went down⁶⁵³.

⁶⁴⁹ Ilves, “The Consequences of Cyber Attacks”.

⁶⁵⁰ Ilves, “The Consequences of Cyber Attacks”.

⁶⁵¹ Cyrus Farivar and Vinton Cerf, “Estonia”, in *The Internet of Elsewhere: The Emergent Effects of a Wired World*, (New Brunswick, New Jersey; London: Rutgers University Press, 2011), 109–49. www.jstor.org/stable/j.ctt5hjgfh.8.

⁶⁵² Farivar and Cerf, “Estonia”.

⁶⁵³ Farivar and Cerf, “Estonia” 136–138.

Estonia was quick to blame Russia for the attacks, and Russia was quick to deny them. In 2007 Russian ambassador Vladimir Chizhov, brushing off the allegations, remarked that “Cyber-space is everywhere”, a tacit reminder of the issues of territoriality and attribution⁶⁵⁴. To this day, one ethnic-Russian Estonian citizen was convicted, but, due largely to the difficulty of attribution, no further charges were pursued.

Of course, the attacks on Estonia did not trigger Article 5, however they did trigger a massive undertaking by NATO to rectify a hitherto inadequate cyber defense apparatus. In 2007, the defence minister of Estonia Jaak Aaviksoo pointed out that “Not a single Nato defence minister would define a cyber-attack as a clear military action at present.”⁶⁵⁵. This changed within years when NATO extended the weight of Article 5 to cyberspace.

Conclusion and Final Remarks

To summarize, NATO’s Article 5 commits members of the alliance to mutual defense if one is subject to an “armed attack.” The language remains vague enough to allow for flexibility, however if invoked this could complicate efforts within the alliance to come to agreement. The article has only been invoked once and would only be invoked in case of a “serious” cyberattack, which to this point has not been concretely defined. In the aftermath of a cyberattack, issues of attribution, proportionality and territoriality could further complicate matters. Attribution is exceedingly difficult to ascertain with a high degree of accuracy, proportionality has seen little precedent, and territoriality is nebulous in cyberspace.

When pondering what constitutes a “serious” cyberattack, it is tempting to wonder if an attack similar in scale to the 2007 attacks in Estonia took place, would it trigger Article 5? The answer is most likely not. While NATO has taken a sharper public stance against cyberthreats, the issue of

⁶⁵⁴ Ian Traynor, “Russia accused of unleashing cyberwar to disable Estonia”, *The Guardian*, May 16, 2007, accessed August 17, 2020, <https://www.theguardian.com/world/2007/may/17/top-stories3.russia>.

⁶⁵⁵ Traynor, “Russia accused of unleashing cyberwar”.

attribution makes it unreasonable to mobilize forces in response. In any case, considering how rapidly cyberspace has evolved and expanded in recent decades, it would not be unreasonable to anticipate some “serious” cyberattack in the future, whatever it may look like.

Article 5 continues to symbolize the collective defense agreed upon by the member states of NATO, however its exceedingly rare invocation coupled with the logistical issues of countering cyberattacks make it highly unlikely that it will be triggered. Nevertheless, NATO serves a critical purpose in cyber defense and should continue to bolster its efforts through the CCD COE and strengthen the cybersecurity systems used to protect the physical, logical, and social infrastructure of NATO and its member states.

How Gun Policies Between The United States of America and the European Union Affect Modes of Violence Used by Far-Right Groups

McKenzie KOTARA

Abstract: The overall purpose of this paper is to explore the gun policies between the United States of America and the European Union in order to gain an understanding of how these policies might affect what modes of violence are used by far-right groups between the two regions. This research was conducted through extensive literature and data review from several different sources, such as the TESAT report and use of data from the Center for Strategic and International Studies. In this paper, we find that guns policies do not affect the modes of violence used by far-right groups between the United States and the European Union, even though the two have extremely different policies when it comes to the use and possession of firearms.

Keywords: guns, gun policies, far-right, US, EU

Introduction

This paper compares the gun policies in the United States and the European Union to determine whether the gun policies affect the modes of violence used by far-right extremists. To explore this, this paper looks at the gun policy in the United States, including the individual states of Texas, New York, and Nevada to show how gun policies may differ within the country. The same procedure is used to examine the gun policy of the European Union, and also looks at the gun policies of individual member states of Germany and France to gain an understanding of how policies may differ among the member states of the European Union.

After the analysis of the gun policies of both the United States and the European Union, the author looks into modes of violence used in previous attacks by far-right extremists, such as the use of guns in the Walmart Shooting in El Paso, Texas, and the use of incendiary devices in the bombing of the Alfred P. Murrah Federal Building in Oklahoma City.

With less gun control in the United States than in the European Union, this paper hypothesizes that stricter gun policies lead to the use of less firearms in far-right attacks. By making it harder to gain possession of firearms, this paper posits that it may deter violence through the use of guns. This topic is critical to research and analyze because according to the Global Terrorism Index, “incidents of far-right terrorism have been increasing in the West”⁶⁵⁶, thus meriting looking into the modes of violence used to gain a better understanding of exactly what kind of violence may be on the horizon.

The Far-Right in the West

The United Nations Security Council’s Counter-Terrorism Committee Executive Directorate recently proclaimed the far-right posing as a threat that is

⁶⁵⁶ “Global Terrorism Index 2019: Measuring the Impact of Terrorism”, Institute for Economics & Peace. Sydney, November 2019. Available from: <http://visionofhumanity.org/reports> (accessed August 2020).

not only growing but also becoming increasingly transnational⁶⁵⁷. The category of ‘far-right’ is influenced by many factors that create many different factions, groups, and movements, such as white supremacy, Christian identity adherents, those concerned with the apocalypse, important strands of libertarianism, emergency preparedness, and paleoconservative⁶⁵⁸. There are also many different definitions of the far-right. For the purpose of being consistent, we use the definition from the Global Terrorism Index (GTI) of 2019 which states that “‘far-right’ refers to a political ideology that is centered on one or more of the following elements: strident nationalism (usually racial or exclusivist in some fashion), fascism, racism, anti-Semitism, anti-immigration, chauvinism, nativism and xenophobia”⁶⁵⁹. However, not every person, group, or movement that holds one or more of these elements is necessarily considered far-right.

Furthermore, it is important to point out that there are two sides to the far-right: those who use democratic, conventional ways in order to sway politics, and those that use violence to get their political ideologies across and influence politics with an aim for “revolutionary change”⁶⁶⁰. This paper examines those who use violence, in what is referred to as right-wing terrorism violence (RTV). Right-wing terrorism can be defined as “the use of threat of violence by sub-national or non-state entities whose goals may include racial or ethnic supremacy; opposition to government authority; anger at women, including the involuntary celibate (or ‘incel’) movement; and outrage against certain policies, such as abortion”⁶⁶¹. Most of the far-right attacks in Europe have been committed by individuals not groups⁶⁶².

⁶⁵⁷ “Member States Concerned by the Growing and Increasingly Transnational Threat of Right-wing Terrorism”, United Nations, Accessed August 13th, 2020. https://www.un.org/sc/ctc/wp-content/uploads/2020/04/CTED_Trends_Alert_Extreme_Right-Wing_Terrorism.pdf.

⁶⁵⁸ Jacob Aasland Ravndal, “Explaining right-wing terrorism and violence in Western Europe: Grievances, opportunities and polarization”, *European Journal of Political Research*, 15 (2018): 847.

⁶⁵⁹ “Global Terrorism Index 2019”, Institute for Economics & Peace.

⁶⁶⁰ Ravndal, “Explaining right-wing terrorism and violence in Western Europe”: 847.

⁶⁶¹ Catrina Doxsee, Nicholas Harrington, Seth G. Jones, “The Tactics and Targets of Domestic Terrorists”, Center for Strategic and International Studies, July 2020: 2.

⁶⁶² Doxsee, Harrington, Jones, “The Tactics and Targets of Domestic Terrorists”: 2.

Scholars such as Jacob Aasland Ravndal claim the motivation behind right-wing terrorist violence in Northern Europe includes a combination of “high immigration, low electoral support for anti-immigration (radical right) parties,...extensive public repression of radical right actors and opinions...”, while in Southern Europe it consists of a “combination of socioeconomic hardship, authoritarian legacies, and extensive left-wing terrorism and militancy.”⁶⁶³ These conditions, or ‘recipes’, as Ravndal refers to them, are also met with a third condition for allowing RTV – significant polarization between far-right activists and all those that they consider or view as their enemies⁶⁶⁴.

As for the United States, there are far-right groups that define themselves as militias whose goals are to “reinvigorate the traditional republican institution of the amateur citizen soldier as a counter to the anti-democratic and ‘tyrannical’ dimensions of the contemporary federal government”⁶⁶⁵.

In Germany, specifically in Dresden November 2019, ABC News reported a “Nazi Emergency”, referring to an increase in right wing extremism⁶⁶⁶. A citizen’s organization *Pegida*, which stands for “‘Patriotic Europeans against the Islamization of the West’”, has also experienced an increase in their membership numbers with thousands of supporters showing their loyalty and support by participating in marches⁶⁶⁷. Alongside of these trends, we see the rise in different far-right political parties such as Golden Dawn in Greece, and Alternative for Deutschland in Germany and paramilitary groupings throughout the European Union.

In addition to taking part in violent events, far-right groups also participate in demonstrations. In Germany in 2015 for example, there were

⁶⁶³ Ravndal, “Explaining right-wing terrorism and violence in Western Europe”,: 846.

⁶⁶⁴ Ibid.

⁶⁶⁵ Jonathan Obert, Elias Schultz, “Right Wing Militias, Guns, and the Technics of State Power”, Law, Culture, and the Humanities, vol. 16(2): 238.

⁶⁶⁶ Sarah Haca, “30 years after the fall of the Berlin wall, right-wing extremism is on the rise as the East lags behind”, abc News, accessed August 7th, 2020. <https://abcnews.go.com/International/30-years-fall-berlin-wall-wing-extremism-rise/story?id=66670250>.

⁶⁶⁷ Haca, “30 years after the fall of the Berlin wall, right-wing extremism is on the rise as the East lags behind”

690 right-wing extremist rallies⁶⁶⁸. By coming together in rallies, it enables them to show ‘power through numbers’, and support for the ideals that they adhere to. Typically, “80–85% of all rallies dealt with the issues of asylum, immigration, and islamization”, representing specific areas the far-right groups devote their attention to⁶⁶⁹.

From 2015 to present in America, individuals and religious institutions have been the main targets of right-wing attacks. Individuals have predominantly been targeted due to racial motivations, with attackers using firearms as their primary weapon. Previously in 1994, the main targets of RTV were abortion-related, with 27% of all attacks carried out on women’s health clinics and the medical staff. However, since 1994 to present, there has been a growing trend of individual’s targeted because of their ethnic, racial, or religious background, including the religious institution that they may have been associated with⁶⁷⁰.

Guns and Gun Rights in America

This part will focus on: Nevada, New York and Texas in order to show the spectrum of gun regulation in the USA.

As stated by Obert and Schultz, “to say that gun rights are a defining feature of American public life is stating the obvious”⁶⁷¹. In the United States, the Pew Research Center found that “three in ten American adults say they personally own a gun, and an additional 11% say they live with someone who does”⁶⁷², illustrating that guns and gun ownership are commonplace

⁶⁶⁸ “Right-wing extremism” Bundesamt für Verfassungsschutz, accessed August 12th, 2020. <https://www.verfassungsschutz.de/en/fields-of-work/right-wing-extremism/figures-and-facts-right-wing-extremism/right-wing-extremist-demonstrations-2015>.

⁶⁶⁹ “Right-wing extremism”, Bundesamt für Verfassungsschutz.

⁶⁷⁰ Doxsee, Harrington, Jones, “The Tactics and Targets of Domestic Terrorists”: 3.

⁶⁷¹ Jonathan Obert, Elias Schultz, “Right Wing Militias, Guns, and the Technics of State Power”, Law, Culture, and the Humanities, vol. 16(2): 236.

⁶⁷² John Gramlich, Katherine Schaffer, “7 facts about guns in the U.S”, Pew Research Center, accessed August 10th, 2020. <https://www.pewresearch.org/fact-tank/2019/10/22/facts-about-guns-in-united-states/>.

in the United States. Although most gun owners use their guns for activities such as target practice, hunting, and general recreation, others use them for protection – either from someone or the government infringing upon their rights as an American citizen.

As the Second Amendment of the United States Constitution affirms:

*“A well-regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed”*⁶⁷³.

Many Americans still hold the right to bear arms as their sacred right that the government must not infringe upon. In recent years, the US Government has debated and some attempts have been made to push for greater gun controls following many deadly events involving guns such as the shooting at Sandy Hook Elementary School and the shooting at a Walmart in El Paso, Texas. However, the resistance and protests by many Americans with their proclaimed right to bear arms has prevented any drastic changes or reforms⁶⁷⁴.

When examining right-wing terrorist violence, the right to bear arms in the US is of particular interest. Members of the far-right that belong to militia movements in America view guns as the “ultimate guarantors of freedom”⁶⁷⁵. Although RTV does not always include gun violence, the Global Terrorism Index points out how “over the past four decades, one in every five mass shootings in the US has been classified as a terrorist attack”, thus showing a need to look into gun policy.

Those on the far right in America, at least those part of militia movements such as the Oath Keepers and the Three Percenters, view the current American government as “a collapse of the vision of the founders, as a creation of an alien, non-democratic form of politics dedicated to stripping power from citizens”⁶⁷⁶. The push for gun control in the country has further reinforced

⁶⁷³ US Const. Amend II.

⁶⁷⁴ Roland Hughes, US gun debate: Four dates that explain how we got here, BBC. Accessed: December 14th, 2020: <https://www.bbc.com/news/world-us-canada-42055871>.

⁶⁷⁵ Obert, Schultz, “Right Wing Militias, Guns, and the Technics of State Power”: 237.

⁶⁷⁶ Ibid.

the belief that it is up to them to rise up against the current government and also teach self-sufficiency through activities such as hunting⁶⁷⁷.

When Barak Obama was elected president, the militia movement in America saw a revival (after it slowed during the 1970s), brought about with concerns over his race, fears that somehow he was involved in “Muslim extremism”, and “supposed expansions of federal authority via the Affordable Care Act and the financial services bailout” which were perceived as crises⁶⁷⁸. The overall goal of militia movements was to fight against any tyranny as well as “protecting the homeland”⁶⁷⁹.

Militias perceive themselves as the last line of defense to protect the rights of people from the encroachment of the government. Specifically, they focus protecting theirs and others rights to bear arms. When surveyed, “two thirds of gun owners say that [protection] is a major reason why they own a firearm”, aside from reasons of hunting, collection of firearms, and for work purposes⁶⁸⁰. This does not speak entirely for the whole of the far-right spectrum, but the concerns and worries of perceived crises of the militia movement are commonly held in the far-right amongst many other groups and organizations.

Each state in the United States has their own gun policies. In Nevada’s State Constitutional Provision Article 1, Section 11, Paragraph 1 for example, it states, “Every citizen has the right to keep and bear arms for security and defense, for lawful hunting and recreational use and for other lawful purposes.”⁶⁸¹. Nevada maintains a broad interpretation on what guns may be used for, leaving it up to citizens, as long as laws in place are followed.

Meanwhile in New York, the State’s Constitutional Provision states nothing. However, Article 2, Section 4 of the New York Civil Rights Law states,

⁶⁷⁷ Ibid: 246.

⁶⁷⁸ Obert, Schultz, “Right Wing Militias, Guns, and the Technics of State Power”: 239.

⁶⁷⁹ Ibid: 240.

⁶⁸⁰ Gramlich, Schaeffer, “7 facts about guns in the U.S”.

⁶⁸¹ NRA-ILA. *nd*. “State Gun Laws”. Accessed August 11th, 2020. <https://www.nraila.org/gun-laws/state-gun-laws/>.

"A well-regulated militia being necessary to the security of a free state, the right of the people to keep and bear arms cannot be infringed."⁶⁸². New York has no provision, but their Civil Rights Law mirrors the Second Amendment almost completely.

As for Texas, the State's Constitutional Provision states in Article 1, Section 23, "Every citizen shall have the right to keep and bear arms in the lawful defense of himself or the State; but the Legislature shall have power, by law, to regulate the wearing of arms, with a view to prevent crime."⁶⁸³. The Constitution defines defense as the main reason for the use of gun, either for oneself or the State. However, the Constitution also makes it clear that the State has the power to regulate gun use to ensure that it is only used for purpose of defense as well as deter crime"⁶⁸⁴.

Gun Rights in the European Union

In the European Union, states share the belief that the bearing of firearms should be restricted⁶⁸⁵. More specifically, "within the EU a shared understanding exists whereby possession and use of firearms should be limited to state authorities and access to firearms by the public should be restricted"⁶⁸⁶. The European Union prohibits the following firearms: fully automatic weapons and military weapons, explosive military missiles and launchers, firearms disguised as other objects, and ammunition with penetrating, explosive or incendiary projectiles, and the projectiles for such ammunition.

Firearms in the European Union that are subject to authorization include eight types of weapon: 1) firearms used by marksmen or hunters, 2) semi-automatic or repeating shot firearms, 3) single-shot firearms with center-fire

⁶⁸² Ibid.

⁶⁸³ Ibid.

⁶⁸⁴ NRA-ILA. *nd*. "State Gun Laws".

⁶⁸⁵ Erica Bowen, Becky Crookes Sue Elliott, F. Jeane Gerard, Mike Hellenbach, Helen Poole, Thanos Stamos, "The detection and policing of gun crime: Challenges to the effective policing of gun crime in Europe", *European Journal of Criminology*, vol.15(2) (2018): 172.

⁶⁸⁶ Bowen, Crookes, Elliott, Gerard, Hellenbach, Poole, Stamos, "The detection and policing of gun crime";: 174.

percussion, 4) single-shot firearms with rim-fire percussion whose overall length is less than 28cm, 5) semi-automatic long firearms whose magazine and chamber can together hold more than three rounds, 6) semi-automatic long firearms whose magazine and chamber cannot together hold more than three rounds, where the loading device is removable or where it is not certain that the weapon cannot be converted, with ordinary tools, into a weapon whose magazine and chamber can together hold more than three rounds 7) repeating and semi-automatic long firearms with smooth-bore barrels not exceeding 60 cm in length, and 8) semi-automatic firearms for civilian use which resemble weapons with automatic mechanism⁶⁸⁷.

As for firearms that are subject to declaration, this category includes firearms used by hunters, long firearms with single-shot rifled barrels, single-shot short firearms with rim-fire percussion whose overall length is not less than 28cm, repeating long firearms other than those described by types 6 above, and semi-automatic long firearms other than those in numbers 4 through 7 above⁶⁸⁸. Firearms that have no restrictions include single-shot long firearms with smooth-bore barrels⁶⁸⁹.

Amongst member states of the European Union, there exists “significant variation” when it comes to firearm policies such as in Croatia, Portugal, Spain, the Netherlands, Denmark, Germany, Belgium, France, Sweden, and Italy⁶⁹⁰. I will analyze the individual policies of Germany and France in particular because they are two countries that experience a higher number of right-wing terrorist and general terrorist violence, as seen by the attacks in Hanau, Halle, and on mosques after the Charlie Hebdo attack.

In Germany there are some of the most stringent gun policies in the world⁶⁹¹. The minimum age for possession of any type of firearm is

⁶⁸⁷ Ibid: 175.

⁶⁸⁸ Ibid.

⁶⁸⁹ Bowen, Crookes, Elliott, Gerard, Hellenbach, Poole, Stamos, “The detection and policing of gun crime”,; 175.

⁶⁹⁰ Ibid: 174.

⁶⁹¹ Frank Gardner. “Germany Shooting: ‘Far-right extremist’ carried out shisha bars attack”, BBC, August 14th, 2020. <https://www.bbc.com/news/world-europe-51567971>.

18 across the board. However, when assessing policies on individual types of firearms, the restrictions range significantly⁶⁹². When it comes to handguns for example, individuals must have a license which enables them to possess only two of them⁶⁹³. With long guns, citizens are limited to only three semi-automatic long guns, and “pump action shotguns with pistol grips or a short overall length are prohibited”. It does not specify however whether a license is required⁶⁹⁴. Concerning both air guns and gas and alarm weapons, licenses are required. In the case of small firearms, individuals are required to carry a permit, and can be obtained without having to show any expert knowledge⁶⁹⁵.

As for in France, the minimum age requirement of 18 only applies to handguns and long guns. For handguns, a license holder may possess up to seven 22 calibre guns, or five handguns of a larger calibre⁶⁹⁶. To possess long guns, a psychological exam is required, and a license holder may have no more than twelve firearms as well as no more than fifty rounds of ammunition⁶⁹⁷. In the case of gas and alarm weapons, they are freely available if the firepower for the weapon is less than two joules, and air guns do not require a license if a person’s gun is less than ten joules of projectile energy or more than two⁶⁹⁸.

In addition to individual member state restrictions, the European Union, since 2015, developed a firearms directive that adds further measures to make it more difficult to acquire firearms⁶⁹⁹. In 2016 the European Parliament came to an agreement that a revision of the original firearms direc-

⁶⁹² Bowen, Crookes, Elliott, Gerard, Hellenbach, Poole, Stamos, “The detection and policing of gun crime”,: 178.

⁶⁹³ Ibid.

⁶⁹⁴ Ibid.

⁶⁹⁵ Ibid.

⁶⁹⁶ Ibid.

⁶⁹⁷ Ibid.

⁶⁹⁸ Bowen, Crookes, Elliott, Gerard, Hellenbach, Poole, Stamos, “The detection and policing of gun crime”,: 178.

⁶⁹⁹ “Firearms Directive”. European Commission, accessed August 12th, 2020. https://ec.europa.eu/growth/sectors/firearms_en.

tive was needed to increase the security of citizens⁷⁰⁰. The changes made to the original firearms directive included a ban of certain semi-automatic firearms such as automatic firearms that can be changed into semi-automatics, long semi-automatics (with a length less than 60cm), and long semi-automatics that had loading devices of more than ten rounds, and short semi-automatic firearms with loading rounds that had more than twenty rounds⁷⁰¹.

The revised firearms directive of 2016 also includes a regulation on acoustic weapons and alarm and signal weapons. Acoustic weapons were declared to still be “used in theaters or movies, subject to declaration, authorization, or license depending on the category they belong to before transformation”⁷⁰², meaning that these inactive weapons may still be used, so long as they have been declared, are licensed or authorized, and correspond with the type of firearms they had been when they were active. Along with this, the revised directive planned to treat museums and collectors of firearms as “any civilian firearms holder”⁷⁰³ and will “have the possibility to acquire category A firearms”⁷⁰⁴, but they may only do so under strict conditions⁷⁰⁵.

As with acoustic weapons, deactivated weapons must also be declared and include stricter enforcement of deactivation rules. Furthermore, stricter conditions for the online acquisition of firearms and clearer rules on marking them have been put in place to improve the capability of tracing weapons. Finally, European Union countries require medical checks for the authorization in acquiring a firearm⁷⁰⁶.

As this analysis has demonstrated, there exists a significant range between the United States and the European Union. In the case of the EU, there are

⁷⁰⁰ Ibid.

⁷⁰¹ Ibid.

⁷⁰² Ibid.

⁷⁰³ Ibid.

⁷⁰⁴ Ibid.

⁷⁰⁵ Ibid.

⁷⁰⁶ European Commission. “Firearms Directive”.

significantly more restrictions when it comes to purchasing as well as possessing guns. Despite the restrictions in the EU, they are still widely used in right-wing attacks, as seen by the shootings at the Halle Synagogue and in Hanau in Germany. Although, this does not by any means say that guns are the only primary weapon of right-wing extremists.

Modes of Violence Used by Right-Wing Extremists in The United States and the European Union

Over the past decade, there has been a surge in right-wing terrorism⁷⁰⁷. With an increase in right-wing politically motivated violence, it is important to examine what modes of violence are being used for attacks, and at what rates. Statistics from the Center for Strategic and International Studies (CSIS) show that in America firearms are overwhelmingly the main weapon of choice in fatal attacks with firearms being the primary weapon of fatal attacks 73% of the time between 2005 and 2020⁷⁰⁸. The question that remains is why firearms remain an attractive weapon of choice when committing acts of terror? Perhaps it is the limited restrictions and availability of guns in the United States compared to other countries and regions.

Despite the popularity of firearms in fatal terror attacks, CSIS statistics found incendiary devices as the weapon of choice at 38% in non-fatal attacks compared to firearms at only 24% between 2005 and 2020⁷⁰⁹. However, in fatal attacks, incendiary devices were used only 4% of the time⁷¹⁰. The report goes on to identify other weapons used in fatal far-right terrorist attacks and found melee weapons (generally knives or other sharp weapons) were 20% and 3% were vehicles⁷¹¹. The report concludes that there

⁷⁰⁷ "Global Terrorism Index 2019: Measuring the Impact of Terrorism", Institute for Economics & Peace, Sydney, November 2019. Available from: <http://visionofhumanity.org/reports> (accessed August 2020).

⁷⁰⁸ Doxsee, Harrington, Jones, "The Tactics and Targets of Domestic Terrorists": 4.

⁷⁰⁹ Ibid.

⁷¹⁰ Ibid.

⁷¹¹ Ibid.

have been four identified modes of violence used in fatal far-right terrorist attacks: melee, incendiary devices, firearms, and vehicles, of which firearms were used at the highest rate⁷¹². As the report demonstrates, guns are not the *only* mode of violence used, nor will they likely ever be.

As for the European Union, groups often train for their attacks as paramilitary do by including mixed martial arts, survival training, and marksmanship⁷¹³. Although there is limited data on exactly how often firearms are used in far-right attacks in the European Union, research suggests firearms play an important role in the training of far-right groups⁷¹⁴. Research by EU Terrorism Situation and Trend Report (TESAT) reported groups in Czech Republic, Hungary and Belgium all include the possession and use of firearms in their training. Furthermore, the report goes on to note that some Eastern European Countries receive “visits by Belgian right-wing extremists... for the purpose of training or self-defense and marksmanship”⁷¹⁵. The frequency of the inclusion of firearms in training illustrates their importance.

Although there are stark differences between the USA and EU on their gun policies, both regions view guns of significant importance in far-right groups. In the United States, we find that guns are used the majority of the time in fatal right wing attacks, while in the European Union, they are used more in the training of far-right groups, which could lead to greater use in attacks committed in the European Union in the near future.

Conclusion

In this paper the author explored who the far-right are in the West, with the special focus on the US and the EU and their modes of violence used

⁷¹² Ibid.

⁷¹³ “European Union Terrorism Situation and Trend Report 2020”, European Union Agency For Law Enforcement Cooperation 2020, June 23rd, 2020 (Accessed September 27, 2020) <https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020>.

⁷¹⁴ Ibid.

⁷¹⁵ Ibid.

when committing violent and terroristic acts. The specific gun policies of the United States of America and the European Union were also discussed, which showed that the European Union has more restrictions on guns than in the United States. In terms of the modes of violence used by the far-right, this paper found firearms as the primary weapon the majority of the time in fatal terrorist attacks, and incendiary devices as second. When discussing the far-right in the West, this paper found private individuals were the main targets due to racial motivations, as well as their religious affiliation.

Although the information found and presented is not sufficient to come to any definitive conclusion about whether or not gun policies between the regions affect the modes of violence used by far-right extremists in their attacks, we can confirm that guns are the primary weapon of attacks in the United States because of their high availability and protection in the country. We also discovered in the case of the European Union that despite of strict gun regulations in the region, guns are still often used in right-wing attacks. More research is still needed, especially that the most recent trends⁷¹⁶ show an increase in right wing extremism. Thus, overall, there is little evidence that suggests that differing gun policies affect the modes of violence used by the far-right in violent attacks.

⁷¹⁶ Violent Right-Wing Extremism and Terrorism –Transnational Connectivity, Definitions, Incidents, Structures and Countermeasures, Report by Counter-Extremism Project. November 2020. Accessed December 14th, 2020. https://www.counterextremism.com/sites/default/files/CEP%20Study_Violent%20Right-Wing%20Extremism%20and%20Terrorism_Nov%202020.pdf.

The Relation Between the Refugee Crisis, Terrorism, and Far-right Extremism in Europe

Sami SHIHADAH

Abstract: This paper examines how terrorist groups have capitalized on the immigration and refugee crisis. First the paper looks at the possible threat of European ISIS fighters returning back to Western European countries under the guise of asylum seekers. Then the paper looks at the rise of terrorism in Europe; evaluates possible outcomes of this crisis or any possible future one, and provides recommendations to mitigate immigration processes without compromising international security.

Keywords: Terrorism, ISIS, Immigration, Refugees, European Union, Extremism

Introduction

Throughout history, humankind witnessed different tragedies that led to forced displacement in such as the Great Famine in the United Kingdom, World War II, the Holocaust, the Partition of India, and currently the ongoing Syrian civil war, which has caused the forced displacement of more than 5.6 million refugees around the globe and another 6.2 million people displaced within the country⁷¹⁷. Massive waves of refugees and asylum seekers collapsed the capacity of United Nations High Commissioner

⁷¹⁷ Harriet, Sherwood. "The Guardian". the Guardian, May 5, 2019. <https://www.theguardian.com/technology/2019/may/05/airbnb-homelessness-renting-housing-accommodation-social-policy-cities-travel-leisure>. August 22, 2020.

for Refugees (UNHCR), World Food Program (WFP), and the United Nations (UN) to provide help to those people in need. The majority of those refugees are living in terrible and inhuman conditions. Many refugees seek a better life with a dignified future in the European Union (EU), even if it means risking their life by crossing the Mediterranean Sea illegally on a rubber boat. This crisis involving immense waves of refugees crossing into EU borders has provided both far-right radicals and jihadists the perfect terrain to commence their terrorist attacks. In the case of far-right oriented political parties, it has served as a suitable excuse to grow their base and get the ball rolling towards their zero-immigration policies and overtaking Europe's power.

Despite the dramatic situation of the refugees and the European countries' noble gesture by welcoming the staggering numbers of refugees, the whole process should be monitored and controlled to avoid the infiltration of Syrian regime war criminals, ISIS fighters, and other radicals among the innocent people. Furthermore, European policies should enforce the eradication of any radicalization of the far-right movements or religious-oriented extremism to avoid any future attacks that will cost innocent lives.

This paper examines how terrorist groups have capitalized on the immigration and refugee crisis in Europe, with a particular focus on France and Germany as case studies since Germany hosted the highest numbers of immigrants and refugees since the international refugee crisis in 2015, and France suffered the highest casualties due to religious-oriented terrorist attacks. First this paper looks at the possible threat of European ISIS fighters returning to Western European countries under the guise of asylum seekers. Then the paper looks at the rise of terrorism in Europe. The paper then proceeds by evaluating possible outcomes of this crisis or any possible future ones, and concludes by providing recommendations to mitigate immigration processes without compromising international security.

The Relation Between Terrorism and the Refugee Crisis

Prior to the onset of the waves of terror attacks in 2014, Europeans already had violent images of jihadist and extremist engraved in their memories following the attacks in Europe – the *Pan Am Flight 103*⁷¹⁸, also known as the Lockerbie attack that caused 259 victims; the *Saint-Michel*⁷¹⁹ subway bombing in Paris, leaving four dead and over 150 injured; Spain's worst-ever terrorist attack, also known as 11M⁷²⁰ attacks that killed 192 and injured more than 1800 in Madrid's simultaneous bombing; and Oslo⁷²¹ attacks, where an anti-Muslimism extremist killed 77 people.

Europeans could not imagine that these haunting memories would come back and that a new wave of terror attacks would be knocking on their door, threatening their lives and their loved ones in such a brutal and surprising way. On May 24, 2014, the world was overwhelmed by the brutal images of a jihadist attacker opening fire on the Jewish Museum⁷²² visitors in Brussels, killing four of them. The attacker – jihadist *Mehdi Nemmouche*⁷²³, was considered the first ISIS returnee⁷²⁴ fighter to carry on a religious-oriented attack in Europe. It also represented a new phenomenon of a second or third generation Muslim immigrant who had become

⁷¹⁸ Federal Bureau of Investigation. "Remembering Pan Am Flight 103", December 14, 2018. <https://www.fbi.gov/news/stories/remembering-pan-am-flight-103-30-years-later-121418>.

⁷¹⁹ Alan, Riding, ed. "EXPLOSION KILLS 4 AND INJURES MANY ON TRAIN IN PARIS". *NYTimes*, July 26, 1995. <https://www.nytimes.com/1995/07/26/world/explosion-kills-4-and-injures-many-on-train-in-paris.html>.

⁷²⁰ "EL PAÍS: El Periódico Global". *EL PAÍS*, March 12, 2004. https://elpais.com/diario/2004/03/12/espana/1079046001_850215.html.

⁷²¹ Elisa, Goodman, Mala J. David. "At Least 80 Dead in Norway Shooting". *NYTimes*, July 22, 2011. <https://www.nytimes.com/2011/07/23/world/europe/23oslo.html>.

⁷²² News, BBC. "Brussels Fatal Gun Attack at Jewish Museum". BBC News, May 24, 2014. <https://www.bbc.com/news/world-europe-27558918>.

⁷²³ "Mehdi Nemmouche", n.d. <https://www.counterextremism.com/extremists/mehdi-nemmouche>.

⁷²⁴ WIRES, NEWS. "Brussels Jewish Museum Shooter 'an Angry French Teen' Who Was Radicalised in Jail". France 24, March 8, 2019. <https://www.france24.com/en/20190308-brussels-jewish-museum-attack-mehdi-nemmouche-french-teen-radicalised-jail>.

radicalized in Europe, later traveled to join ISIS in Syria and Iraq, and return to Europe to carry out future terror attacks. This newer phenomenon has escalated the fears and suspicions towards immigrants of Arab or Muslim origins as being either affiliated with and/or a returnee fighter of ISIS.

Brussels Jewish Museum strike unleashed a series of terrorist attacks causing hundreds of deaths and injuries that will hurt Europeans for generations. A few months after the Brussels attack, several Jihadists stormed *Charlie Hebdo*⁷²⁵ offices, killing multiple artists, journalists, and even an unarmed Muslim police officer. This deadly attack was intended to demonstrate the power of ISIS and its jihadist terrorist, capable of striking Europe at any cost, even if it meant killing Muslims as was the case of the Muslim police officer. It is considered the most symbolic attack against the West and its freedom of speech, as Charlie Hebdo is a satirical magazine known for its controversial caricatures and had been threatened by jihadist groups for years. The terrorists were identified as second-generation Muslim immigrants who were born, raised, and radicalized in Paris⁷²⁶. This event raised questions and concerns regarding the capacity of European law enforcement to protect Europe's cities from any future attacks. It also aided far-right groups in spreading their theories and conspiracies of the Islamization⁷²⁷ of Europe and enlarging its fan base.

In 2014 the humanitarian crisis in Syria already began, however, the international community largely ignored it until 2015 when the iconic photo of Aylan Kurdi⁷²⁸ – a three year infant who tragically died while attempting to cross with his father from Turkey to Greece, began circulating social media triggering moral outrage and demands for something more to be

⁷²⁵ Dan, Bilefsky, and Maïa, De La Baume. "Terrorists Strike Charlie Hebdo Newspaper in Paris, Leaving 12 Dead". NYTimes, January 7, 2015. <https://www.nytimes.com/2015/01/08/world/europe/charlie-hebdo-paris-shooting.html>.

⁷²⁶ Angelique, Chrisafis. "The Guardian". The Guardian, January 12, 2015. <https://www.theguardian.com/world/2015/jan/12/-sp-charlie-hebdo-attackers-kids-france-radicalised-paris>.

⁷²⁷ Lena, Krikorian. "Islamisation of Europe: Myth or Reality? – Polemics". Polemics, March 1, 2018. <http://www.polemics-magazine.com/dasicon2018/islamisation-europe-myth-reality>.

⁷²⁸ Diane, Cole. "Study: What Was The Impact Of The Iconic Photo Of The Syrian Boy?", January 13, 2017. <https://www.npr.org/sections/goatsandsoda/2017/01/13/509650251/study-what-was-the-impact-of-the-iconic-photo-of-the-syrian-boy>.

done. Europe decided to open its borders and host a substantial number of refugees seeking safety and shelter; Angela Merkel announced that Germany⁷²⁹ would open its gates to all refugees and take the largest percentage of the newcomers. This initiative however was not well received by far-right groups, triggering a physical attack against running mayor *Henriette Reker*⁷³⁰, causing her life-threatening wounds because of her support for refugee and immigration policies. The attacker was later identified as Frank. S⁷³¹, a German citizen who later pleaded guilty and confessed to the attack due to her pro-refugee stance.

Not long after the European initiative of hosting refugees, Paris once again under attack by jihadist radicals that perpetrated synchronized attacks across the French capital, killing more than 130 citizens and injuring hundreds. One of the synchronized attacks took place in the Stade de France⁷³², where the national teams of France and Germany were celebrating a soccer match with the presence of the heads of state. The ISIS bombers detonated their suicide vests in the stadium entrance, demonstrating that if they successfully managed to enter the stadium, they could easily and efficiently target the highest-ranking officials of the French government wherever and whenever they planned to⁷³³. While investigating the attack, French authorities discovered a Syrian passport that allegedly belonged to one of the bombers. The authorities then tracked back the data from the

⁷²⁹ Allan, Hall, and, John Lichfield. "Germany Opens Its Gates: Berlin Says All Syrian Asylum-Seekers Are Welcome to Remain, as Britain Is Urged to Make a 'Similar Statement.'" *The Independent*, August 24, 2015. <https://www.independent.co.uk/news/world/europe/germany-opens-its-gates-berlin-says-all-syrian-asylum-seekers-are-welcome-to-remain-as-britain-is-10470062.html>.

⁷³⁰ Adam, Chandler. "German Mayoral Candidate Henriette Reker Wounded in Anti-Immigrant Attack". *The Atlantic*, October 17, 2015. <https://www.theatlantic.com/international/archive/2015/10/germany-cologne-mayor-attack-henriette-reker/411139/>.

⁷³¹ (www.dw.com), Deutsche Welle. "Man Who Stabbed Mayor of Cologne Sentenced to 14 Years in Jail | DW | 01.07.2016". DW.COM. Accessed August 29, 2020. <https://www.dw.com/en/man-who-stabbed-mayor-of-cologne-sentenced-to-14-years-in-jail/a-19371698>.

⁷³² Jamie, Cleland, and Ellis, Cashmore. "Nothing Will Be the Same Again After the Stade de France Attack: Reflections of Association Football Fans on Terrorism, Security and Surveillance". *Journal of Sport and Social Issues* 42, no. 6 (December 2018): 454–69. doi:10.1177/0193723518797028.

⁷³³ Daniel L. Byman, "Beyond Iraq and Syria: ISIS' Ability to Conduct Attacks Abroad". *Brookings*, June 8, 2017. <https://www.brookings.edu/testimonies/beyond-iraq-and-syria-isis-ability-to-conduct-attacks-abroad/>. September 28th, 2020.

passport making the astonishing discovery that Ahmad Al-Mohammed⁷³⁴ had been a refugee who had arrived in Europe through Leros⁷³⁵ amongst other refugees during the crisis.

The authenticity of the passport and the attacker's identity however remain in question, as the document could have been counterfeited to stage the narrative of the attacks. As was later discovered, the real Ahmad Al-Mohammed was allegedly a soldier in the Syrian regime forces who was captured and killed by ISIS in the Syrian war⁷³⁶. Notwithstanding the French authorities official statement, far-right politicians and fanatics across Europe have embraced the conspiracy that the terrorist attack in Paris on November 13, 2015, was carried out by Syrian refugees that arrived in Europe during the recent immigration crisis⁷³⁷. Therefore, the expression of facts divulges that the refugee crisis is not the main reason behind the rise of jihadist terror attacks in Europe, but it did contribute to the recent rise of far-right parties and extremism in Europe⁷³⁸.

⁷³⁴ Peter, Bergen, and David, Sterman, Alyssa Sims, and Albert Ford, eds. "THE SEVERE THREAT TO EUROPE". JSTOR, 2016. <https://www.jstor.org/stable/resrep10494.7>.

⁷³⁵ Ahmad Al-Mohammed: Fingerprints now reveal that TWO of the Paris suicide bombers had entered Europe through Greece a month before the attacks: Anthony, Joseph., "Fingerprints Reveal 2 of the Paris Suicide Bombers Entered Europe through Greece". Daily Mail, November 21, 2015. <https://www.dailymail.co.uk/news/article-3327928/Fingerprints-reveal-TWO-Paris-suicide-bombers-entered-Europe-Greece-month-attacks.html>.

⁷³⁶ The New York Times. "Syrian Passport by Stadium Stolen or Fake, A.F.P. Reports", November 17, 2015. <https://www.nytimes.com/live/paris-attacks-live-updates/syrian-passport-reportedly-was-stolen-or-fake/>.

⁷³⁷ Richard, Wike, Stokes, Bruce and Katie Simmons. "Europeans Fear Wave of Refugees Will Mean More Terrorism, Fewer Jobs". *Pew Research Center's Global Attitudes Project*, July 11, 2016. <https://www.pewresearch.org/global/2016/07/11/europeans-fear-wave-of-refugees-will-mean-more-terrorism-fewer-jobs/>.

⁷³⁸ Andreas, Steinmayr. "Did the Refugee Crisis Contribute to the Recent Rise of Far-Right Parties in Europe?" *ECONSTOR.EU*. Accessed October 2, 2020. <https://www.econstor.eu/bitstream/10419/181257/1/dice-report-2017-4-50000000000857.pdf>.

European Social and Political Reaction to Staggering Waves of Immigrants

History books are filled with examples and images of massive immigration waves such as in World War II, the Holocaust, second Sudanese civil war, and Rohingya persecution in Myanmar, to name a few. Images of people fleeing their hometowns towards an unknown path should serve as a potent reminder and lesson to never allow such tragic events occur again. However, humankind seems to tragically forget. With all the new technologies making almost any desired information accessible by one click, the creation of the UN, WFO, and UNHCR to prevent any armed conflicts, global hunger, and to support refugees and asylum seekers around the world, humankind is still not prepared to face any global humanitarian crisis appropriately. Countries like U.S., Canada, and European countries that form the free world are still struggling with the differentiation between legal and illegal immigration, forgetting the past that affected most of them and even forced a portion of their population to flee wars and disasters – giving politicians from different political ideologies the opportunity to label immigrants and refugees according to their interests. Far-right politicians converted the newcomers as a threat to their national security and social integrity, fueling the fanatic's radicalization to the point of incentivizing them to perpetrate terrorist attacks against immigrants, refugees, and anyone who sympathizes with them.

Border control by Frontex⁷³⁹ and European intelligence agencies in collaboration with the UN should increment its filtering process and enforce its policies to protect the EU from any possible future threat. European Parliament and states should enforce social policies to ensure the integration of the newcomers into the society, preventing social unrest and disturbances as happened with the blockade⁷⁴⁰ across the Bulgarian and Greek borders in 2016, to prevent the entry of any refugees.

⁷³⁹ Fabrice, Leggeri, ed. "Foreword". Accessed September 2, 2020. <https://frontex.europa.eu/about-frontex/foreword/>.

⁷⁴⁰ Jakarta Globe. "Europe's Refugee Blockade", February 23, 2016. <https://jakartaglobe.id/multimedia/europes-refugee-blockade/>.

Gigantic migration waves irritate different parts of the society of any host country, due to the rejection of such an unfamiliar phenomenon, and could perceive it as a threat. Especially when the political leaders encourage such ideas through their political campaigns and the influence of foreign disinformation campaigns as the Russian Federation is actively conducting against European countries, especially Germany during the past few years⁷⁴¹. In Germany, since Chancellor Angela Merkel opened the doors for the asylum seekers and refugees, different parties have prioritized the immigration crisis and dominated political discussions. Over the course of one year, over 1.3⁷⁴² million people entered Germany and applied for asylum in the country in 2015. Along with the data available, the crime rate and terrorist attacks in Europe increased significantly since 2014. For example, in Germany 6.1 million offenses were reported in 2014, and in 2016, 6.4 million offenses were reported, marking a difference of 300,000 offenses in just two years. German men between the ages of 14 and 30 form 9% of the country's population and yet have committed half the crimes rate in Germany⁷⁴³. Also, since 2014 proportion of non-German suspects in the crime statistics has increased from 24% to just over 30%⁷⁴⁴. The increased crime rate in Germany can be related to the surge in numbers of refugees. And this fact has been exploited by an aggressive massive political campaign carried out by anti-refugee European parties led to a general decline in the acceptance of the new arrivals among the European population. Further fueled by aggressive Russian disinformation campaign, exaggerating and even creating "fake news" to create a parallel reality, in which Europe will face Armageddon due to migration – portraying the immigrants and refugees as the evil force that will soon destroy the

⁷⁴¹ Gustav Gressel. "Russia's Hybrid Interference in Germany's Refugee Policy". ECFR. European Council on Foreign Relations, February 4, 2016. https://www.ecfr.eu/article/commentary_russias_hybrid_interference_in_germanys_refugee_policy5084.

⁷⁴² Pew Research Center's Global Attitudes Project. "Number of Refugees to Europe Surges to Record 1.3 Million in 2015", August 2, 2016. <https://www.pewresearch.org/global/2016/08/02/number-of-refugees-to-europe-surges-to-record-1-3-million-in-2015/>.

⁷⁴³ Reality Check. "Are Migrants Driving Crime in Germany?" BBC News, September 13, 2018. <https://www.bbc.com/news/world-europe-45419466#:~:text=In%202014%2C%20German%20men%20between,seekers%20who%20came%20in%202015.>

⁷⁴⁴ Ibid.

“weak” European countries. The fake testimonies created by the Russian disinformation campaigns such as the case of the Russian speaking victim Lisa that alleged she was raped by several refugees in Germany, serves as a great example. However, this incident never happened, and the fake story was dispersed through different anti-refugee social media groups and websites such as Anonymous.Kollektive and Asylterror.com⁷⁴⁵.

Since the 2015 refugee crisis, the political party Alternative für Deutschland (Alternative for Germany: Alternative für Deutschland, AfD) grew their base and empowered their vision. During the summer of 2015, many Germans seemed to welcome refugees arriving in the country, but the mood changed by 2016, when a majority of Germans wanted a cap placed on refugees⁷⁴⁶. This change among the German people regarding the acceptance of more asylum seekers and new arrivals immigrants is due to the unfortunate events that stormed the Old World, causing hundreds of deaths and injured thousands, tearing apart thousands of families in the deadliest wave of terrorist attacks in decades in addition to the aggressive disinformation campaigns influencing over the perception of the German society. According to Europol, in the period of (2014–2016) 561⁷⁴⁷ terrorist attacks failed or foiled across the European continent, and the law enforcement conducted 2823 arrests during the same period targeting possible terrorists from both religiously motivated jihadists and far-right radicals.

AfD⁷⁴⁸ is by far the best known opponent to Merkel’s pro-refugee policy. AfD seeks to eliminate the number of immigrants entering the country with their zero-immigration policy; hence the party is also seeking the German borders to eradicate the unregulated illegal immigration. In France, the leader

⁷⁴⁵ Jakub, Janda. “The Lisa Case STRATCOM Lessons for European States”. *Security Policy Working Paper* No.11/2016 (January 1, 2016): 1/4.

⁷⁴⁶ Jeffrey, Gedmin. “Right-Wing Populism in Germany: Muslims and Minorities after the 2015 Refugee Crisis”. Brookings, July 24, 2019. <https://www.brookings.edu/research/right-wing-populism-in-germany-muslims-and-minorities-after-the-2015-refugee-crisis/>.

⁷⁴⁷ “Terrorism Situation and Trend Report”. TE SAT EUROPOL, 2017.

⁷⁴⁸ Deutsche Welle. “AfD: What You Need to Know about Germany’s Far-Right Party | DW | 28.10.2019”. DW.COM. Accessed August 30, 2020. <https://www.dw.com/en/afd-what-you-need-to-know-about-germanys-far-right-party/a-37208199>.

of the far-right National Front (NF, fr. Front National)⁷⁴⁹, Marine Le Pen, led the party and secured 27.7% of the vote nationally, situating the party in the front of the political scene in France. 16% of those who voted for the NF said they had changed their voting intentions after the November 13th attacks⁷⁵⁰. A clear statement that reflects the success of the far-right to ride the wave of the anti-refugees and immigrants' movements, especially after the jihadist terror attacks.

The violent far-right extremists started taking its rage against refugees themselves by attacking everyday refugee camps across Germany. More than 1,600 crimes against refugees and asylum-seekers in their temporary or permanent shelters caused them physical harm, destroyed their personal belongings and even burned down the entire buildings. These attacks took place in 2019 only⁷⁵¹. German authorities admitted that the refugees could expect to be attacked at any moment and everywhere, a statement that demonstrates a drastic rise in far-right hostility against the asylum-seekers. What many feared in Europe, was the return of the far-right extremists in the European streets, who have gained a voice among a large majority of the population who is full of anger and uncertainty, fueled by the economic crisis, disagreement with the EU policies, and the ongoing crisis that has brought millions of foreigners blamed for all the terrorist attacks happening across Europe.

Recommendations on Policies and Solutions to Facilitate Immigration Without Compromising National Security

The UN and UNHCR should increase their capacity to process asylum petitions for refugees already located in countries hosting refugees temporarily. The

⁷⁴⁹ Financial Times. "France's National Front Taps into Rising Anti-Immigrant Mood", September 6, 2015. <https://www.ft.com/content/62131206-5473-11e5-8642-453585f2cfd>.

⁷⁵⁰ Michel, Rose. "French Parties Scramble to Halt Rise of Far-Right National Front". Reuters, December 7, 2015. <https://www.reuters.com/article/us-france-politics/french-parties-scramble-to-halt-rise-of-far-right-national-front-idUSKBN0TQ0T820151207>.

⁷⁵¹ Deutsche Welle. "Germany: More than 1,600 Crimes 'targeted Refugees and Asylum-Seekers' | DW | 27.03.2020". DW.COM. Accessed August 30, 2020. <https://www.dw.com/en/germany-more-than-1600-crimes-targeted-refugees-and-asylum-seekers/a-52935715>.

current process to relocate asylum petitioners can take up to two years, and excludes many stranded refugees that can lead to dangerous security risks and loss of lives. To illustrate one example, a former Syrian intelligence officer⁷⁵² found a safe haven in Germany after fleeing Syria and claiming asylum. He was later identified by a former detainee that previously had been tortured by him in Damascus. After their incredible encounter between the alleged war criminal and his former detainee in a supermarket, the victim informed the German authorities, leading them to open an investigation and arrest the individual. This incident is considered the first international Syrian war crime, which is also a point of concern, as it revealed the possibility of a large numbers of war criminals arriving in Europe among the refugee waves⁷⁵³.

Processing immigrants and border control are complicated tasks during peace or regular times for any state and its law enforcement agencies. It requires many resources that prove difficult to provide when used at its maximum capacity in extraordinary cases such as the refugee crisis in 2015. For this reason it is necessary to have a broad intrastate cooperation between European intelligence agencies and Frontex to share and improve its database that includes information gathered during the process of collecting intelligence of possible threats, and used as a primary filter to decline the entry and the arrest of individuals that could pose a risk to European and international security.

During the interview of an asylum petition, candidates should provide valid information and relevant documentation besides their narrative about their past and the reason behind their asylum application. Authorities should look into the smallest details and contrast it with existing databases as well as to seek help from current or former refugees to validate it. European authorities should share the information collectively, instantly be able to access databases that include the collected information to create a list of matching individuals from the narratives that could potentially be involved

⁷⁵² Deborah Amos, "Syrian War Crimes Trial Resumes In Germany", *NPR*, May 21, 2020, <https://www.npr.org/2020/05/21/859991380/syrian-war-crimes-trial-resumes-in-germany>.

⁷⁵³ Ben Hubbard, "Germany Takes Rare Step in Putting Syrian Officers on Trial in Torture Case". *The New York Times*, April 23, 2020, <https://www.nytimes.com/2020/04/23/world/middleeast/syria-germany-war-crimes-trial.html>.

in crimes against humanity, and to avoid their infiltration among other asylum seekers as was the case in Netherlands and Germany.

Besides the importance of information, technology is a crucial factor in the War on Terrorism and seeking international security. Therefore, European authorities should seek viable facial recognition software⁷⁵⁴ and artificial intelligence to process millions of images and footages that are published on different websites to identify potential radicals, terrorists, and criminals before they reach Europe.

Conclusion

The world has witnessed how far-right extremists and jihadists have taken advantage of security gaps, the most recent being the refugee crisis in 2015. While the European countries face hundreds of thousands of refugees seeking shelter and safety, far-right politicians adapt to events and circumstances that favor their ideology, and grasp onto any theory, even if part of a foreign disinformation campaign, so long as it fuels their base and helps them reach their goal. The European Union is confronted with the challenging task of maintaining the security and stability within its border to avoid the repetition of any terrorist attack. Social unrest could lead to the radicalization of some individuals that are considered far-right fanatics and enforce its security and policies to mitigate the complexity of the immigration process without compromising its national security. The author believes that authorities need to cooperate with non-profit organizations and citizens' initiatives to avoid such scenarios.

⁷⁵⁴ Adonis, Hoffman. "Facial Recognition Could Stop Terrorists before They Act | TheHill". *The Hill*, March 9, 2020. <https://thehill.com/opinion/technology/486570-facial-recognition-could-stop-terrorists-before-they-act>.

The Role of Disinformation in Migration: Case Studies of the United States and Sweden

Marianne PERKINS

Abstract: Fake news, junk news, disinformation, and countermedia are distinct from similar terms like misinformation due to their intentionality to mislead. Disinformation has existed for centuries, but its forms today in the information age are especially dangerous with the possibility of high levels of amplification on social media. The characteristics of democratic elections – such as in the United States 2016 presidential election – may very well be changed by the increase in and specialization of echo chambers filled with like-minded individuals and often also disinformation. These echo chambers result in increased polarization with little resolve and many countries confused as to what is the solution to fighting disinformation. Mitigation strategies are possible and necessary for individuals and countries to win the so-called information war.

Keywords: Disinformation, misinformation, fake news, migration, immigration, United States of America, Sweden

Introduction

Fake news and disinformation dominate social media or at least are perceived to. These now ever present issues seem to be a recent invention of the information age, although both have existed since the start of humanity in various forms⁷⁵⁵. In fact, the 1896 American presidential election

⁷⁵⁵ Richard Stengel, *Information Wars: How We Lost the Global Battle Against Disinformation & What We Can Do About It* (New York: Atlantic Monthly Press, 2019), 3.

spawned perhaps one of the first written and widely circulated forms of actual fake news in the creation of the newspaper known as *The Commoner*. In the wake of his defeat in the presidential election to William McKinley, William Jennings Bryan chose to create *The Commoner* to go against the mainstream media, which he deemed as biased and unreliable. The creation of the newspaper's biased and misleading content caused newspapers throughout the United States to raise concern over the blatant lies and fake news *The Commoner* spread⁷⁵⁶. Eventually this turn of the century fake news subsided, but in recent years there has been a reemergence in the discussion and spread of fake news and disinformation similar to Jennings Bryan's early twentieth century newspaper.

What is new about today's disinformation is the way it is able to be increasingly weaponized through the internet and social media to become a new form of warfare. Information warfare is beginning to be combined with traditional warfare to create asymmetric conflicts like the 2014 Russian annexation of Crimea⁷⁵⁷. Russian trolls used social media in Ukraine and state controlled news like RT to mobilize dissent and create an image of western interference in any anti-annexation protests. While for many westerners this type of asymmetric warfare was unimaginable, the Russian Federation had become quite skilled in propagating and spreading disinformation from its Soviet past and present commitment to continue to influence local and far-away issues⁷⁵⁸. Foreign and domestic sources are both capable and willing of achieving their goals—to mobilize, to disorganize, and to confuse—through the use of disinformation. The political nature of the lion's share of disinformation focuses on salient issues, which may cause interference in democratic elections and may affect state policy negatively.

This paper presents an overview about the phenomenon of disinformation. Two case studies have been analyzed with the special focus on the

⁷⁵⁶ Adrienne Lafrance, "How the 'Fake News' Crisis of 1896 Explains Trump", *The Atlantic*, January 19, 2017, accessed August 13, 2020. <https://www.theatlantic.com/technology/archive/2017/01/the-fake-news-crisis-120-years-ago/513710/>.

⁷⁵⁷ Yevgeniy Golovchenko, "Using Social Network Analysis to Understand Disinformation on Social Media", Sage Publications Ltd., 2019, accessed August 7, 2020, doi:10.4135/9781526498632.

⁷⁵⁸ Stengel, *Information Wars*, 145.

issue of migration, in order to demonstrate how the use of disinformation can jeopardize stability and security of democratic states.

Previous Research and Theory

Fake news today exists with an entirely different meaning than it was originally intended in the recent past. Prior to circa 2015, fake news existed merely to describe political satire like *Saturday Night Live* and *The Daily Show with Jon Stewart*⁷⁵⁹. An Israeli study found that exposure to comedic fake news caused increased cynicism in the surveyed individuals as the comedic portrayals of politicians were viewed as fairly accurate. When this exposure to comedic news was combined with higher levels of hard news like factually based newspapers and television programming, the surveyed individuals were able to be somewhat less cynical as the fake news portrayals of politicians were judged more accurately based on the characteristics and behaviors of the real politicians from their hard news exposure⁷⁶⁰. Although this previous knowledge of fake news and its effects are able to be better understood through this previous research, the new version of this term is still young with its difficulty to track and often inability to establish causation and not simply correlation.

The current definition of fake news – understood as “false stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke”⁷⁶¹ – emerged in 2014 with Craig Silverman as he was researching disinformation at Columbia University. When beginning his career at BuzzFeed⁷⁶², he started to use the term

⁷⁵⁹ Regina Marchi, “With Facebook, Blogs, and Fake News, Teens Reject Journalistic ‘Objectivity,’” *Journal of Communication Inquiry* 36, no. 3 (July 2012): 253, accessed August 7, 2020, doi:10.1177/0196859912458700.

⁷⁶⁰ Meital Balmas, “When Fake News Becomes Real: Combined Exposure to Multiple News Sources and Political Attitudes of Inefficacy, Alienation, and Cynicism,” *Communication Research* 41, no. 3 (April 2014): 442, accessed August 10, 2020, <https://doi.org/10.1177/0093650212453600>.

⁷⁶¹ Cambridge Dictionary definition of the term “fake news,” <https://dictionary.cambridge.org/pl/dictionary/english/fake-news>, accessed December 15, 2020.

⁷⁶² “About BuzzFeed,” <https://www.buzzfeed.com/about>, accessed December 15, 2020.

in his work. By early 2017, the term was adopted and used by American president Donald Trump to describe CNN and their coverage on his presidency⁷⁶³. Over time, this term has shifted and is now used by politicians and the general population to describe certain types of news, especially news which one does not agree with. Using this politically charged term often leads to polarization⁷⁶⁴. Due to the politicization of the term, some scholars are electing to shift from the term fake news to instead call this phenomenon countermedia. According to Hopp, Ferrucci, and Vargo, the term countermedia more accurately defines this phenomenon as the news in question is more often than not news with some limited truth present. The content in countermedia, aside from the “grain of truth”, is designed to be politically charged by presenting news with a distinct narrative. Countermedia’s goal is to push a particular narrative and interpretation, making the denotation of fake news, countermedia, and disinformation essentially the same⁷⁶⁵.

Aside from these three essentially equivalent words, there must be a clear distinction between the terms misinformation, disinformation, and malinformation. These terms exist on a spectrum with misinformation and malinformation being the two extremes and disinformation lying somewhere in the middle. Malinformation describes the release of personal information with the intent to harm⁷⁶⁶. Often at times the issue of releasing information is simply due to its purpose to blackmail a person, but it can be used, for example, politically with an attack on a particular politician.

⁷⁶³ Andrew Beaujon, “Trump Claims He Invented the Term ‘Fake News’ – Here’s an Interview With the Guy Who Actually Helped Popularize It”, *The Washingtonian*, October 2, 2019, accessed August 9, 2020, <https://www.washingtonian.com/2019/10/02/trump-claims-he-invented-the-term-fake-news-an-interview-with-the-guy-who-actually-helped-popularize-it/>.

⁷⁶⁴ Anthony J. Gaughan, “Illiberal Democracy: The Toxic Mix of Fake News, Hyperpolarization, and Partisan Election Administration”, *Duke Journal of Constitutional Law & Public Policy* 12, no. 3 (2017): 75, accessed August 13, 2020, <https://scholarship.law.duke.edu/djclpp/vol12/iss3/3>.

⁷⁶⁵ Toby Hopp, Patrick Ferrucci, and Chris J Vargo, “Why Do People Share Ideologically Extreme, False, and Misleading Content on Social Media? A Self-Report and Trace Data-Based Analysis of Countermedia Content Dissemination on Facebook and Twitter”, *Human Communication Research* (May 2020): 2, accessed August 9, 2020, <https://doi.org/10.1093/hcr/hqz022>.

⁷⁶⁶ Shawn Walker, Dan Mercea, and Marco Bastos, “The disinformation landscape and the lockdown of social platforms”, *Information, Communication & Society* 22, no. 11 (August 2019): 1532, accessed August 8, 2020, doi:10.1080/1369118X.2019.1648536.

The other two terms, misinformation and disinformation, both cover inaccurate claims. However, misinformation lacks the intentionality of disinformation. Disinformation is the “intentional distribution of fabricated information to advance political narratives.”⁷⁶⁷ This intentionality is what makes disinformation, countermedia, and fake news so dangerous.

Today disinformation is increasingly used in an online environment, as shown in the 2016 American presidential election⁷⁶⁸. All social media sites provide internet users – domestic and international actors, the opportunity to create disinformation and share it online, whether it be for profit or for personal gain⁷⁶⁹. The 2016 American presidential election saw a high volume of disinformation from domestic actors and Kremlin-backed trolls. Interestingly however, a significant amount disinformation originated from a small city in Macedonia, where locals worked to sensationalize and plagiarize American alt-right media into new content, which was then promoted on Facebook for profit as opposed to personal investment in the victory of Trump⁷⁷⁰. The reasoning for attention to and interaction with these sensationalized, unbelievable stories was not necessarily due to the Americans steadfast belief in these stories. Rather, as Hermida discusses, social media is simply “an expression of identity”, and sometimes these identities are accidentally or intentionally expressed with disinformation⁷⁷¹. For some people, articles containing disinformation may be viewed as entertaining or even shocking, while for others, they “confirm” what one “always knew.” This explanation exemplifies echo chambers⁷⁷² ability to flourish on social media⁷⁷³.

⁷⁶⁷ Walker, Mercea, and Bastos “The disinformation landscape”, 1532.

⁷⁶⁸ Laura Asperholm Hedlund, “Identifying and Understanding Anti-Immigration Disinformation: A case study of the 2018 Swedish national elections” (PhD diss., Swedish Defence University, 2019), 2019, 10, accessed August 4, 2020, <http://www.diva-portal.org/smash/get/diva2:1324745/FULLTEXT01.pdf>.

⁷⁶⁹ Gaughan, “Illiberal Democracy”, 60.

⁷⁷⁰ Emma Jean Kirby, “The city getting rich from fake news”, *BBC News* online, December 5, 2016, accessed August 8, 2020, <https://www.bbc.com/news/magazine-38168281>.

⁷⁷¹ Ibid.

⁷⁷² Ammol Rajan, “Do digital echo chambers exist?”, *BBC News online* March 4 2019, accessed December 14, 2020, <https://www.bbc.com/news/entertainment-arts-47447633>.

⁷⁷³ Alfred Hermida, “Alfred Hermida Discusses Social Networks and Misinformation”, SAGE Publications Ltd., 2019, accessed August 7, 2020, doi:10.4135/9781526492210.

Echo chambers are becoming increasingly common and perhaps even more specialized to a person's particular beliefs on social media websites like Facebook and Twitter⁷⁷⁴. A 2017 study of 783 Facebook and Twitter users, consisting of a nearly even male/female representation of U.S. citizens, 18 years or older, were selected to participate in a study about sharing disinformation online, defined in this study as countermedia for the validity of the partially true but skewed content. The individuals were also asked to rate themselves on a political scale of one to seven, with one being the most liberal and seven being the most conservative. The study found that the majority of shares of countermedia were on Facebook, with 1,152 posts being shared by the participants. Only 129 instances of disinformation, again from the same group of individuals, were shared on Twitter⁷⁷⁵. Although most of the participants did not share any countermedia, the study found those identifying themselves as extremely liberal or extremely conservative (those classifying themselves as a one or a seven) shared disinformation the most. On Facebook, the most conservative individuals shared 26% of the countermedia with the most liberal sharing 17.5%. These statistics showed on Facebook 22.97% of the participants shared 43.4% of the total countermedia shared. While this study is not conclusive on the spread of disinformation on social media concerning elections or politics, it does show an increased rate of sharing disinformation by hyper-partisan individuals⁷⁷⁶.

Mainstream Media Distrust and Disinformation about Migration

The role of mainstream media has been rapidly changing since the advent of the internet and social media. Mainstream media is no longer able to serve as a "gatekeeper" with the ability to prevent misleading or untrue news⁷⁷⁷. Today almost anyone can create and share content such as ama-

⁷⁷⁴ Hopp, Ferrucci, and Vargo, "Why Do People Share Ideologically Extreme", 18.

⁷⁷⁵ Ibid., p. 10–15.

⁷⁷⁶ Ibid., p. 18–23.

⁷⁷⁷ Gaughan, "Illiberal Democracy", 59.

teur journalists. This enables individuals to serve as whistleblowers and to cover important events and developments that may be ignored by mainstream news outlets. At the same time, it allows anyone to post false and misleading content on social media without the need to gain permission from a media outlet or authority figure. This was exemplified in the lead up to the 2016 American presidential election, whereby disinformation alleging a high amount of voter fraud was allowed to spread⁷⁷⁸. A study by Silverman on behalf of BuzzFeed confirmed this and noted the rise of fake news versus mainstream media shared on Facebook⁷⁷⁹ in the days leading up to American 2016 presidential election. He discusses how the type of news—fake and mainstream—shared on social media about the American 2016 presidential election shifted between February 2016 until election day in November, whereby fake news eventually outpaced mainstream media shortly before and on election day⁷⁸⁰. Although causation cannot be established, the findings do suggest that the decrease of the share of mainstream media and increase of the fake news may have had a political influence on voters.

While fake news represents one threat, the lack of media freedom to publish content freely serves as another. Recently the Freedom House has reported a general global decline in media freedom in recent years, posing a significant threat to democracies, especially for emerging ones such as in Africa and Asia⁷⁸¹. Despite the United States receiving the highest and best possible score for media freedom, many Americans have increasingly grown skeptical of mainstream news in the past few years, calling for the rise of alternative news sources and an increase in reliance on the social media to locate these sources. In 2018, *Gallup* carried out a survey reporting that 41%

⁷⁷⁸ Ibid., 59.

⁷⁷⁹ Craig Silverman, “This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook”, *BuzzFeed News*, November 16, 2016, accessed August 13, 2020, <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>.

⁷⁸⁰ Ibid.

⁷⁸¹ Sarah Repucci, “Media Freedom: A Downward Spiral”. *Freedom House*, 2019, accessed August 7, 2020, <https://freedomhouse.org/report/freedom-and-media/2019/media-freedom-downwardspiral>.

of the respondents trusted the media – Democrats more than Republicans and Independents⁷⁸². Despite this seemingly low number, American trust in the mass media has actually increased. In 2016 for example, only 32% of Americans trusted mainstream media, a record low for this survey⁷⁸³. These numbers show a serious divide in the trust in the mainstream media, most starkly when comparing Democrats and Republicans, with 69% of the former and only 15% of the latter trusting in the mass media in 2018. Although the exact cause is unknown, partisan politics and a view of a lack of representation of conservative viewpoints in mainstream news certainly may play a large part in Republican mistrust of mainstream media.

The reason for Republican mistrust in the media may be connected to political ideology and politicians such as President Trump who use divisive policies e.g. the border wall as well as “Muslim ban” rhetoric⁷⁸⁴. While North America and Europe have varying degrees of right-wing populism, political parties and politicians subscribing to this ideology are present in a number of these states. Germany’s Alternative for Germany party, Sweden’s Alternative for Sweden party, the United States’ President Trump, Poland’s Law and Justice (Prawo i Sprawiedliwość, PiS) party, and Brazil’s President Jair Bolsonaro are just a few examples⁷⁸⁵. These examples are by no means exhaustive, but they do show a few notable examples of the spread of right-wing populism in North America, Europe, and even Latin America. In general, these parties are built on the concept of a past with cultural homogeneity and/or economic success with an “us vs. them” mentality. The “them” can be anything from elites, Muslims, individuals

⁷⁸² Megan Brennan, “Americans Trust in Mass Media Edges Down to 41%”, *Gallup* online, September 26, 2019, accessed August 8, 2020, <https://news.gallup.com/poll/267047/americans-trust-mass-media-edges-down.aspx>.

⁷⁸³ Art Swift, “American’s Trust in Mass Media Sinks to New Low”, *Gallup* online, September 14, 2016, accessed August 8, 2020, <https://news.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx>.

⁷⁸⁴ Jessica Goudeau, “Refugee Resettlement is Close to Collapse. That Was Trump’s Plan”, *The New York Times*, July 28, 2020, accessed August 13, 2020, <https://www.nytimes.com/2020/07/28/opinion/us-refugee-resettlement-trump.html>.

⁷⁸⁵ BBC News, “Europe and right-wing nationalism: A country-by-country guide”, November 13, 2019, accessed August 17, 2020, <https://www.bbc.com/news/world-europe-36130006>.

of a different race or culture, migrants and even the media itself⁷⁸⁶. This builds a battle that must be fought to protect “us” from an adversary. Often at times alt-right populist politicians and parties choose multiple and often interconnected battles for change in policy and practice. An excellent example is the United States, which combined “them” to include all migrants, especially Muslims and those from Hispanic and Latino backgrounds⁷⁸⁷. Alt-right populist parties and politicians, especially when they heavily push anti-immigrant policy, enjoy support from their international counterparts, especially Russia due to the divisiveness of these issues⁷⁸⁸.

Migration has proven to be a particularly salient, alt-right populist area of interest due largely in part to the 2015 European migration crisis and the assumed influx of Mexican and other Latino migrants to the United States. The amplification of politicized information on migration is of particular use to Russian trolls and international alt-right organizations to push partisan politics with immigration’s divisiveness⁷⁸⁹. The issue of migration can further be linked, although falsely, to an increase in migration leading to a rise in crime and terrorism causing a divisive stance⁷⁹⁰. Despite the misleading nature of many facts associated with supposed problems arising from migration, they are still able to spread and be widely believed. A call for citizens to react to “save their country from the other” has the potential to be particularly salient in mobilizing voters and individuals by perceiving migrants as a threat to the citizen’s way of life, culture, and religion. Viewing and labelling migrants as “the other” can extend through generations of family members built in the original host country⁷⁹¹.

⁷⁸⁶ Asperholm Hedlund, “Identifying and Understanding Anti-Immigration Disinformation”, 6.

⁷⁸⁷ Thomas Greven, “The rise of right-wing populism in Europe and the United States”, *Friedrich-Ebert-Stiftung* (2016): 1–6, accessed August 8, 2020, https://www.fesdc.org/fileadmin/user_upload/publications/RightwingPopulism.pdf.

⁷⁸⁸ Jonathan Birdwell et al., “Smearing Sweden: International Influence Campaign in the 2018 Swedish Election”, (London: Institute for Strategic Dialogue, 2018), 5, accessed August 8, 2020, <https://www.isdglobal.org/wp-content/uploads/2018/11/Smearing-Sweden.pdf>.

⁷⁸⁹ Birdwell et al., “Smearing Sweden”, 9.

⁷⁹⁰ Magdalena Crisan, “Migration in the Kremlin’s Disinformation War”, *Bulletin of “Carol I” National Defence University* 8, no. 3 (September 2019): 9, accessed August 8, 2020, ProQuest.

⁷⁹¹ *Ibid.*, p. 10.

Additionally, many migrants come from politically and economically unstable environments in which they are unsafe physically and/or economically⁷⁹². These conditions can translate into initial economic instability in their new host country. Migrants are also subject to hate crimes resulting in injury or even death. After a wave of terrorist attacks in early 2016 and a call from then candidate Trump for the Muslim immigration ban, California State University “found that hate crimes against American Muslims were up 78 percent over the course of 2015.”⁷⁹³ The amount of uncertainty for migrants is concerning in every country. The United States has long been held as a welcoming country for immigrants⁷⁹⁴, especially when considering the United States was originally, what then U.S. Senator John F. Kennedy called “a nation of immigrants” in the title of his 1958 book⁷⁹⁵. Disinformation in the United States and internationally threatens the entrance of some of the world’s most vulnerable populations into host states, and even once admitted, there is not a guarantee of safety. While the use of disinformation on migration serves to stop migration, it has at the same time exacerbated the suffering of potential migrants with today’s many humanitarian crises with violent conflicts and wars in their homelands⁷⁹⁶.

Case Studies: The United States of America and Sweden

While many Americans still consider the United States as a “nation of immigrants”, there is a growing number of those who do not, calling for decreased immigration and a border wall. Similarly, Sweden until 2015, was regarded as a country welcoming refuge for migrants, receiving the fourth

⁷⁹² Eduardo Porter and Karl Russell, “Migrants Are on the Rise Around the World, and Myths About Them Are Shaping Attitudes”, *The New York Times*, June 20, 2018, accessed August 15, 2020, <https://www.nytimes.com/interactive/2018/06/20/business/economy/immigration-economic-impact.html>.

⁷⁹³ Eric Lichtblau, “Hate Crimes Against American Muslims Most Since Post-9/11 Era” *New York Times*, September 17, 2016, accessed August 9, 2020, <https://www.nytimes.com/2016/09/18/us/politics/hate-crimes-american-muslims-rise.html>.

⁷⁹⁴ Goudeau, “Refugee Resettlement”.

⁷⁹⁵ John F. Kennedy, *A Nation of Immigrants* (New York: Harper Perennial, 2008).

⁷⁹⁶ Goudeau, “Refugee Resettlement”.

highest number of asylum requests of the OECD countries, following the United States, Germany and Hungary⁷⁹⁷. Today however, the Migration Policy Institute reports that Sweden has taken a more restrictionist policy with the newly elected, nationalist, and anti-immigration government (2018)⁷⁹⁸. The United States has also followed “restrictionist policies following both 9/11 with even more now under the Trump administration, ranging from the Muslim ban to decreased refugee quotas⁷⁹⁹ and a recent attempt to drastically decrease the number of international students studying in the U.S. in July 2020 which was struck down⁸⁰⁰.”

The United States

During Donald Trump’s presidential campaign, he heavily emphasized his anti-migrant sentiments⁸⁰¹ as well as his concern for election fraud resulting from undocumented migrants voting in elections⁸⁰². As a solution to both of these problems, Trump campaigned on populist concepts like “building the wall”, with the wall being along the U.S. border with Mexico in addition to increased deportation⁸⁰³. Almost immediately upon officially becoming the president of the United States, Trump issued his first executive order in January 2017. This executive order was clearly anti-migrant, as it halted the settlement of Syrian refugees, discontinued admission of refugees approved for resettlement, and created the Muslim ban which

⁷⁹⁷ “Inflows of asylum seekers”, OECD International Migration Database and labour market outcomes of immigrants, OECD, accessed September 21, 2020, <http://www.oecd.org/els/mig/keystat.htm>.

⁷⁹⁸ Admir Skodo, “Sweden: By Turns Welcoming and Restrictive in its Immigration Policy”, *Migration Policy Institute*, December 6, 2018, accessed August 13, 2020, <https://www.migrationpolicy.org/article/sweden-turns-welcoming-and-restrictive-its-immigration-policy>.

⁷⁹⁹ Goudeau, “Refugee Resettlement”.

⁸⁰⁰ Nick Anderson and Susan Svrluga, “Trump administration backs off plan requiring international students to take face-to-face classes”, *The Washington Post*, July 14, 2020, accessed August 17, 2020, https://www.washingtonpost.com/local/education/ice-rule-harvard-international-students-rescinded/2020/07/14/319fdae0-c607-11ea-a99f-3bbdff1af38_story.html.

⁸⁰¹ Goudeau, “Refugee Resettlement”.

⁸⁰² Gaughan, “Illiberal Democracy”, 58.

⁸⁰³ Noland D. McCaskill, “Trump promises wall and massive deportation program”, *Politico*, August 31, 2016, accessed August 13, 2020, <https://www.politico.com/story/2016/08/donald-trump-immigration-address-arizona-227612>.

denied entry for citizens from seven Muslim majority countries⁸⁰⁴. This executive order and later cap on refugee admission from 110,000 under the Obama administration to 45,000 in 2017 under the Trump administration broke from the American government's post World War II tradition of welcoming refugees into the United States⁸⁰⁵.

President Donald's Trump's first executive order's focus on migrants—specifically refugees and Muslims—was the first attempt to fulfill his campaign promise of anti-migrant policy⁸⁰⁶. While in office, Trump continues to generate false information and knowingly improbable ideas⁸⁰⁷, such as his idea to relocate undocumented migrants to so called “sanctuary cities”, which are cities choosing to often not comply with assisting Immigration and Customs Enforcement officials with information about potentially undocumented immigrants. Such a transfer, according to Homeland Security, would be impossible due to the high cost and complexity of such a program⁸⁰⁸. Although some unfounded claims do come directly from President Trump, others continue to be generated on social media, even after the 2016 election ended. A recent example from 2018 originated from a post by Twitter user Mike Allen showing a picture of injured and bloodied Mexican police officers. The caption explained this harm was caused by “the caravan”, a term used by Trump to describe asylum seekers from central America seeking refuge in the United States⁸⁰⁹. This post exemplified simultaneously an anti-caravan, pro-Trump, and pro-military interven-

⁸⁰⁴ Goudeau, “Refugee Resettlement”.

⁸⁰⁵ Ibid.

⁸⁰⁶ Miriam Valverde, “Trump's travel restrictions survive Supreme Court, fall short of promised Muslim ban”, *PolitiFact*, November 14, 2018, accessed August 17, 2020, <https://www.politifact.com/truth-o-meter/promises/trumpometer/promise/1401/establish-ban-muslims-entering-us/>.

⁸⁰⁷ Carole McGranahan, “An anthropology of lying: Trump and the political sociability of moral outrage”, *American Ethnologist*, 44, no. 2 (2017): 245, accessed September 21, 2020, <https://doi.org/10.1111/amet.12475>.

⁸⁰⁸ Calvin Woodward and Hope Yen, “AP FACT CHECK: Trump's misleading rhetoric on immigrants”, *AP News*, April 29, 2019, accessed August 13, 2020, <https://apnews.com/fb21a03e4d2246b1926830e-8def6e999>.

⁸⁰⁹ Dan Evon, “Were These Mexican Police Officers Brutalized by Members of a Migrant Caravan?” *Snopes*, October 22, 2018, accessed August 17, 2020, <https://www.snopes.com/fact-check/mexican-police-caravan-photos/>.

tion at the U.S./Mexico border. The truth behind this image has nothing to do with a “caravan” and is in fact a picture from a 2012 student protest in Mexico City⁸¹⁰. This is an excellent example of disinformation in the form of misrepresentation by combining the politically charged caption with the unrelated images.

As a combination of the Trump administration’s anti-migrant stance and fear of election fraud, there have also been attempts on the campaign trail and during his presidency to draw a connection between the two to create a convenient narrative to pursue a political goal. This interconnection supposes that undocumented immigrants vote in elections and skew the vote in favor of the Democratic party⁸¹¹. In 2019, Trump alleged on Twitter thousands of non-citizens voted in Texas elections due to a report published by the Texas Election Commission⁸¹². The Tweet additionally called for increased voter identification laws for elections on the fear that many undocumented immigrants and non-citizens regularly vote in elections. Although the claims made in the Tweet originate from a study, the information used was taken out of context and transformed into a form of disinformation, which journalists later debunked. Alexa Ura explained this report simply flagged voters for citizenship checks, meaning they were not citizens when they applied for and received their state identification cards or driver’s licenses⁸¹³. However, as she points out, non-citizens with green cards or other identification documents, are entitled to become naturalized, and then be eligible to legally vote.

Additionally, Trump spread disinformation and fueled prejudice amongst his supporters about refugee resettlements. Trumps first executive order for example, encouraged a halt to refugee resettlement under the assumption the current process does not vet refugees thoroughly enough

⁸¹⁰ Ibid.

⁸¹¹ Alexa Ura, “Texas officials flag tens of thousands of voters for citizenship checks”, *The Texas Tribune*, January 25, 2019, accessed August 17, 2020, <https://www.texastribune.org/2019/01/25/texas-flags-tens-thousands-voters-citizenship-check/>.

⁸¹² Donald J. Trump, Twitter Post, January 2019, 8:22 a.m., accessed August 13, 2020, <https://twitter.com/realDonaldTrump/status/1089513936435716096>.

⁸¹³ Ura, “Texas officials flag”.

to keep Americans safe. This assumption however is unfounded given that refugees are thoroughly vetted through a process that can take two years or more starting with the United Nations High Commission for Refugees and then again through a thorough vetting process with multiple American governmental agencies, including law enforcement, national security, and intelligence agencies⁸¹⁴. Additionally, the call for the border wall and the necessity of additional law enforcement along the southern border ignores the way the majority of undocumented immigrants arrive in the United States. For the seventh year in a row, the Center for Migration Studies has found visa overstays as the main reason for newly undocumented immigrants. As the Center shares, 62% of newly undocumented immigrant cases are from visa overstays and only 32% of them from illegal border crossings. This finding raises doubts about the need for a border wall and military deployment at the southern border and rather highlights the necessity for increased scrutiny in the Department of State visa approval policy⁸¹⁵.

Sweden

Although Sweden has been receptive of and is a host to a large number migrants, the issue of migration has become a contentious issue in Swedish politics⁸¹⁶. Following the reception of 156,460 asylum requests in 2015, some political parties used this as evidence of a migration crisis in Sweden⁸¹⁷. The two political parties most notable for spreading this idea and fueling fears are the Swedish Democrats (Sverigedemokraterna, SD) and Alternative for Sweden (Alternativ för Sverige, AfS), known for their anti-immigrant beliefs, the AfS being the most extreme⁸¹⁸. While it is not uncommon for political parties to play upon some facts to further

⁸¹⁴ Goudeau, "Refugee Resettlement".

⁸¹⁵ Richard Gonzales, "For 7th Consecutive Year, Visa Overstays Exceed Illegal Border Crossings", *NPR*, January 16, 2019, accessed August 13, 2020, <https://www.npr.org/2019/01/16/686056668/for-seventh-consecutive-year-visa-overstays-exceeded-illegal-border-crossings>.

⁸¹⁶ Birdwell et al., "Smearing Sweden", 9.

⁸¹⁷ OECD, "Inflows of asylum seekers".

⁸¹⁸ Birdwell et al., "Smearing Sweden", 14.

their own political agendas, alt-right parties often manipulate and distort information that is presented in a similar style and format to that of traditional journalism so as to cause confusion and make it difficult for readers to determine what is real or fake news⁸¹⁹. Instead of using the term disinformation, “junk news” is more prevalent in Sweden, although both terms are equivalent – denoting the intention of using misleading news. A study by the Oxford Internet Institute also found that Swedes interact more with “junk news” than other European countries⁸²⁰. Not only is Sweden one of the highest consumers of “junk news” in Europe, it also shares more fake news on Twitter than many other countries, on average eight out of ten times more, most of which are of Swedish origin⁸²¹.

Unlike many countries from Europe and the western world, Sweden has managed to avoid foreign interference and meddling in elections, or so it so far appears. In the 2017 German federal election for example, evidence emerged suggesting that Russian bots were used to spread disinformation, but no such evidence was ever found in Sweden’s 2018 elections⁸²². That is not to say however the Swedish alt-right is entirely isolated from communicating with international alt-right media. One of the starkest examples is the political party Alternative for Sweden, representing a simple alteration to the name of its German equivalent Alternative for Germany. In spite of the apparent connection between the two groups, they remain minimal. This is also the case of European and American alt-right movements that lack coordination and any internationally backed amplification campaigns of disinformation⁸²³.

Despite the lack of coordination between AfS and other alt-right groups, there still has been considerable interest in Sweden amongst international alt-right groups. Although Sweden avoided Kremlin-backed news sources or other alt-right group from meddling in its election by injecting

⁸¹⁹ Asperholm Hedlund, “Identifying and Understanding Anti-Immigration Disinformation”, 12.

⁸²⁰ Birdwell et al., “Smearing Sweden”, 11.

⁸²¹ Asperholm Hedlund, “Identifying and Understanding Anti-Immigration Disinformation”, 4.

⁸²² Birdwell et al., “Smearing Sweden”, 12.

⁸²³ Ibid., p. 26.

disinformation, there existed a disinformation campaign about Sweden for external audiences⁸²⁴. Social media outlets for example portrayed Sweden as “a country in crisis on the verge of a civil and ethnic war”, an assumption drawn from the influx of Muslim migrants to Sweden by alt-right media sources⁸²⁵. The idea that Sweden’s homogeneity was “ruined” circulated despite any evidence to prove this was the case. Even the American broadcast news channel Fox News focused on this supposed issue which was then picked up by President Trump in 2017⁸²⁶. The goal of this smear campaign of disinformation about Sweden was established by Russian-backed media and the alt-right to encourage the emergence of an “anti-liberal” and “anti-migrant” society and policies in Europe and North America⁸²⁷.

Even documentaries emerged out of the international campaign to smear Sweden and spread disinformation about its alleged migration problems. Ami Horowitz’s YouTube mini-documentary “Stockholm Syndrome” gained quite a lot of attention after it was posted to YouTube in December 2016, with some claiming the video sparked Trump’s infamous 2017 comment about “last night” in Sweden⁸²⁸. After the release of the documentary, the majority of the Swedes that were either in the film or filmed the documentary came out and criticized the heavily edited footage. Two policemen interviewed in the documentary also stated that their answers were heavily edited and taken out of context to give the impression that police responses were weak to the supposed increase of violence by migrants⁸²⁹. One of the cinematographers, Emil Marczak, confirmed that

⁸²⁴ Birdwell et al., “Smearing Sweden”, p. 16.

⁸²⁵ Ibid., p. 10.

⁸²⁶ Rick Noack, “Sweden has no idea what Trump meant when he said, ‘You look at what’s happening... in Sweden’”, *The Washington Post*, February 19, 2017, accessed August 13, 2020, <https://www.washingtonpost.com/news/worldviews/wp/2017/02/19/sweden-has-no-idea-what-trump-meant-when-he-said-you-look-at-whats-happening-in-sweden/>.

⁸²⁷ Birdwell et al., “Smearing Sweden”, 17.

⁸²⁸ Noack, “Sweden has no idea”.

⁸²⁹ Hugo Lindkvist, “He filmed the police interview that Trump saw: the material was not edited ethically”, *Dagens Nyheter*, February 23, 2017, accessed August 13, 2020, <https://www.dn.se/kultur-noje/he-filmed-the-police-interview-that-trump-saw-the-material-was-not-edited-ethically/>.

many of Horowitz's questions were manipulated to establish causation between the refugees and a rise in crime⁸³⁰. This attempt to establish a link and release the information in English clearly shows the goal of the entire campaign was to smear Sweden as the creation of disinformation to support an anti-migrant and anti-refugee narrative for the rest of the western world.

Conclusion

Disinformation is an increasingly large adversary in the information age with its ability to stem from a Russian troll factory with non-stop content production or even from a fourteen-year-old in his parent's basement. Anyone can create disinformation to spread on social media, and many may prove to be quite good at it. Its spread is concerning, and its political impact on issues like migration could have lasting impacts to the implosion of government policy and programs. Disinformation resulted in the Trump administration's attack on the American refugee resettlement program that has severely damaged refugee quota caps that could take years to restore and raise again. Without the proper tools to combat the issue of disinformation, the damage to policies and polarization in the years to come could be nearly irreversible.

The 2016 American presidential election showed a worrying creation of a "toxic mix", consisting of the spread of fake news, average broadcast news audiences above 60 years old, and the spread of both good and bad information on the internet that may have the ability to undermine even the strongest democracies⁸³¹. Today, this "toxic mix" continues with little mitigation. Mitigation to the issue of disinformation under a democratic system at times can be viewed as a violation of Freedom of Speech and the First Amendment, and maybe such speculations are correct in certain cases. Nevertheless, mitigation should be attempted. While there are many solutions to combatting disinformation, the most credible avenues

⁸³⁰ Ibid.

⁸³¹ Gaughan, "Illiberal Democracy", 64.

to attempt mitigation are an increase in the availability of fact checking websites, increased research into disinformation detecting Artificial Intelligence (AI), and lastly the introduction of media literacy into curriculum.

The information war against disinformation cannot be simply won by countering every piece of disinformation with the facts directly; instead, it is essential to continuously publish factual information through reliable channels beyond mainstream media⁸³². Mainstream media is most often a source of factual information, but there is a profit motivation to create the most interesting and clicked through stories. It is important for more fact checkers to emerge and to find ways to encourage their use as objective sources. Using fact checkers helps to empower individuals to take disinformation into their own hands to read the facts and choose for themselves how to interpret information. With these fact checkers, it is important to promote their objectivity to prevent them from becoming politically polarized and exacerbating issues. In the future, a fact checker could be artificial intelligence or AI which detects false information. AI can be trained to analyze content using certain key words as well as to distinguish between human networks versus bot networks and use this information to promote facts and disprove or remove disinformation.⁸³³ This advancement would have the ability to stop disinformation from spreading as quickly, but this will only be possible when the AI is able to have an extremely high accuracy level and not remove the content of individuals.

Media literacy for citizens of all ages is essential for a functioning and healthy democracy in the information age. An excellent example is Estonia, which has introduced digital citizenship into school curriculum with a “Lifelong Learning Strategy”⁸³⁴. This curriculum encourages students to be ready in being able to succeed in work and study in today’s digital world. The combination of encouragement to be ready for future career and educational opportunities with an additional emphasis on critical analysis skills allows for students to be ready to also analyze and determine

⁸³² Stengel, *Information Wars*, 172–173.

⁸³³ Stengel, *Information Wars*, 300.

⁸³⁴ Birdwell et al., “Smearing Sweden”, 36.

information to be true, misinformation, or disinformation⁸³⁵. This lifelong education will hopefully remain with students in these types of programs for life, eventually creating a society in which the majority of the population is able to think critically and dissect information for truthfulness. With educational programs, an increase in fact checkers and fact checking technology, it is hopeful that one day polarizing issues such as migration can be analyzed and bipartisan agreement can once again become possible.

⁸³⁵ Ibid., 37.

The Role of Sexual Offenses in Terrorist Activities

Andrew M. HOLUB, Ph.D.

Abstract: The following is intended as an introduction for students and professionals to consider sexual offending within the context of terrorism. Specifically, sexual offending is reviewed as a means of inducing terror (e.g., rape), and as advantageous for recruiting (e.g., access to sexual slaves) and funding (e.g., prostitution) for terrorist organizations. The present analysis is meant to provide a truncated overview rather than a comprehensive examination. Interested readers are directed to other sources for more detailed coverage of topics such as prostitution and terrorism, rape during warfare, terrorism, evolutionary psychology and evolutionary perspectives on terrorism. A report from the United Nations Security Council Counter-Terrorism Committee Executive Directorate⁸³⁶ describes more examples of terrorist organizations recruiting and financing in relation to sexual offenses. The main intent of the present review is to encourage and stimulate future scientific research on sexual offenses and terrorist activities, with specific regard for improving counterterrorism policy and programs.

Keywords: Sexual offending, sexual exploitation, sexual violence, pornography, prostitution, human trafficking, rape, terrorism, evolutionary psychology

⁸³⁶ Counter-Terrorism Committee Executive Directorate, *Identifying and Exploring the Nexus between Human Trafficking, Terrorism, and Terrorism Financing* (New York: United Nations Security Council, 2019), <https://www.un.org/sc/ctc/wp-content/uploads/2019/02/HT-terrorism-nexus-CTED-report.pdf>.

Introduction to Sexual Offending and Terrorism

In order to approach sexual offending in the context of terrorism, first it is necessary to establish working definitions for each. As is true of the study of most human behaviours, both terrorism and sexual offending are broad, heterogenous terms, with numerous, sometimes nebulous definitions. Disparity in definitions of terrorism has become exacerbated by an increase in activities inspired by, but not funded, directed, or otherwise associated with terrorist organizations⁸³⁷ – the problem of the “lone wolf” designation⁸³⁸. It has been suggested that criminal codes should avoid a single monolithic, ultimately incomplete definition of terrorism, and instead embrace multiple definitions that are sensitive to variables that may change based on specific circumstances⁸³⁹. Casting such a wide net may be possible in law, but science requires precision and agreement in definition. For the purpose of the present analysis, terrorism will be understood as: “deliberate, politically motivated use of force or violence (or the threat of violence) with the intention to influence the public opinion through the means of mass communication”⁸⁴⁰. The aforementioned definition includes the role of the media, which may be particularly relevant for sexual offending in the context of terrorism.

Operationalizing “sexual offending” is similarly difficult. “Sexual offending” has been deliberately selected as the term of reference in the present analysis because of its broadness. The term “sexual offending” is most often used in legal statutes, vis-à-vis other criminal behaviours. Generally speaking, if an offense occurs, there must be a norm, rule, law, or other expectation that has been transgressed. Sexual offending is a violation of an established code of conduct regarding sexual behaviour, typically, but

⁸³⁷ Antonia Ward, “How Do You Define Terrorism?” *The National Interest*, May 31, 2018, <https://nationalinterest.org/feature/how-do-you-define-terrorism-26058?nopaging=1>.

⁸³⁸ Bart Schuurman et al., “End of the Lone Wolf: The Typology that Should Not Have Been”, *Studies in Conflict & Terrorism* 42, (2019): 771–778.

⁸³⁹ Alan Greene, “Defining Terrorism: One Size Fits All?” *International and Comparative Law Quarterly* 66, no. 2 (April 2017): 411–440.

⁸⁴⁰ Katarzyna Maniszewska, *Pionierzy Terroryzmu Europejskiego: Frakcja Czerwonej Armii* (Kraków: Apeiron, 2014), 12.

not always, codified by law. Although all countries have laws regulating nonconsensual sexual activities, there are often inconsistencies between countries' penal codes. International humanitarian and criminal law (IHL and ICL, respectively) have sought to fill these voids, with debateable success⁸⁴¹. Numerous international treaties and laws have established conventions regarding violations of human sexual dignity (see International Committee of the Red Cross Customary IHL Database⁸⁴², or United Nations Office on Genocide Prevention and the Responsibility to Protect⁸⁴³ for more information), but even within the piecemeal framework of international agreements, incongruencies remain. For the purposes of the present analysis, "sexual offending" will be understood to include a wide array of behaviours such as "rape, sexual mutilation, sexual humiliation, forced prostitution, and forced pregnancy⁸⁴⁴", pornography, forced abortion, and also a broad list of tactics, such as, blackmail, bribery, deceptive recruitment into marriages/sexual relationships, restriction of movement, use of drugs to remove ability to consent, and other forms of aggression, and violence. In summation, any actual or threatened use of coercion, aggression/violence, or manipulation of consent and personal authority regarding behaviours typical of reproduction, mating, courtship, or romantic relationships can be considered sexual offending. Even this very broad definition likely is not adequately inclusive of the range of behaviours that could be considered sexual offending, but it provides a working basis from which to approach this topic within the context of terrorist activities.

There are countless variables that can predict the perpetration of sexual offenses. The present analysis does not claim to provide an exhaustive review of the causes of sexual offending. Indeed, identifying the causes of sexual offenses has been the subject of volumes of research, from numerous

⁸⁴¹ Keith Suter, "The Successes and Limitations of International Law and the International Court of Justice", *Medicine, Conflict and Survival* 20, (2004): 344–354.

⁸⁴² "Rule 93. Rape and Other forms of Sexual Violence", International Committee of the Red Cross, accessed November 23, 2020, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule93.

⁸⁴³ "Definitions: Genocide, Crimes Against Humanity, War Crimes, and Ethnic Cleansing", United Nations Office on Genocide Prevention and the Responsibility to Protect, accessed November 23, 2020, <https://www.un.org/en/genocideprevention/crimes-against-humanity.shtml>.

⁸⁴⁴ United Nations Women's Rights Unit, "Sexual Violence and Armed Conflict: United Nations Response", *Women2000* (April 1998), <https://www.un.org/womenwatch/daw/public/cover.pdf>.

perspectives and levels of analysis. Similarly, the extent to which sexual offenses are intentionally used by terrorist organizations for the purposes of meeting strategic goals can vary from organization to organization. Although the present analysis focuses on how terrorist organizations can advance their objectives through sexual offending, it must be acknowledged that an individual terrorist may perpetrate sexual offenses for any number of reasons, mirroring the occurrence within the general population. Readers interested in more detailed coverage of sexual offending are directed to a number of more comprehensive resources^{845, 846, 847, 848, 849}.

Attempts to estimate the scope of sexual offending by terrorist organizations has proven extremely difficult. Although most nation states and many international agencies have mechanisms for attempting to track and analyze data regarding sexual offenses, the same apparatus does not exist among and within terrorist organizations. As either actual or prospective non-state entities, terrorist organizations attempt to operate outside of (inter)national law, meaning attempts to document the perpetration of sexual offenses by terrorists are almost certainly deficient, likely underreporting the magnitude and regularity of these activities⁸⁵⁰. Therefore, even if the present report were not constrained by space, lack of available data would render any analysis about the extent of sexual offenses by terrorist organizations incomplete.

This analysis is meant to provide a truncated overview rather than a comprehensive examination. Interested readers are directed to other

⁸⁴⁵ Martin L. Lalumière et al., *The Causes of Rape: Understanding Individual Differences in Male Propensity for Sexual Aggression* (Washington D.C.: American Psychological Association, 2005).

⁸⁴⁶ Amy D. Lykins, ed., *Encyclopedia of Sexuality and Gender*, (Springer Nature Switzerland AG, 2020), <https://doi.org/10.1007/978-3-319-59531-3>.

⁸⁴⁷ William F. McKibbin et al., "Why Do Men Rape? An Evolutionary Psychological Perspective", *Review of General Psychology* 12, (2008): 86–97.

⁸⁴⁸ Thornhill and Palmer, *A Natural History of Rape*.

⁸⁴⁹ Griet Vandermassen, "Evolution and Rape: A Feminist Darwinian Perspective", *Sex Roles* 64, (2011): 732–747.

⁸⁵⁰ Nikita Malik, "Human Trafficking Continues to Be Used by Terrorists: The ICC Must Address It", *Forbes*, June 20, 2019, <https://www.forbes.com/sites/nikitamalik/2019/06/20/human-trafficking-continues-to-be-used-by-terrorists-the-icc-must-address-it/?sh=352e018d230b>.

sources for more detailed coverage of topics such as prostitution and terrorism^{851, 852}, rape during warfare^{853, 854, 855}, terrorism⁸⁵⁶, evolutionary psychology^{857, 858} and evolutionary perspectives on terrorism^{859, 860}.

Finally, it goes without saying that the effects of sexual offenses on victims can be devastating. However, sexual offending can also have ramifications beyond the trauma for individual victims. Sexual offending in the context of terrorist organizations can be considered objectively as a possible means of accomplishing strategic objectives. Adding this superordinate level of analysis to the study of sexual offenses does not ignore the pain and consequences of individual victims, nor the motivations of individual perpetrators; rather it can help provide a deeper understanding of the mechanisms that continue to promote and sustain these behaviours that violate the human dignity of victims (see Conclusions and Future Directions).

⁸⁵¹ Richard J. DiGiacomo, "Prostitution as a Possible Funding Mechanism for Terrorism" (MA thesis, Naval Postgraduate School, 2010).

⁸⁵² Nikita Malik, "Trafficking Terror: How Modern Slavery and Sexual Violence Fund Terrorism", London: The Henry Jackson Society, 2017. <https://henryjacksonsociety.org/wp-content/uploads/2017/10/HJS-Trafficking-Terror-Report-web.pdf>.

⁸⁵³ Dara Kay Cohen, *Rape during Civil War* (Ithaca, NY: Cornell University Press, 2016).

⁸⁵⁴ Randy Thornhill and Craig T. Palmer, *A Natural History of Rape: Biological Bases of Sexual Coercion* (Cambridge, MA: MIT Press, 2000).

⁸⁵⁵ Malcolm Potts and Thomas Hayden, *Sex and War: How Biology Explains Warfare and Terrorism and Offers a Path to a Safer World* (Dallas: BenBella Books, 2008).

⁸⁵⁶ Bruce Hoffman, *Inside Terrorism: Revised and Expanded Edition* (New York: Columbia University Press, 2006).

⁸⁵⁷ Leda Cosmides and John Tooby, "From Evolution to Adaptations to Behavior: Toward an Integrated Evolutionary Psychology", In *Biological Perspectives on Motivated Activities*, ed. Roderick Wong (Norwood, NJ: Ablex, 1995) 10–74.

⁸⁵⁸ David M. Buss, *Evolutionary Psychology: The New Science of the Mind, 6th Edition* (New York: Routledge, 2019).

⁸⁵⁹ Max Taylor, Jason Roach, and Ken Pease, eds., *Evolutionary Psychology and Terrorism*. (New York: Routledge, 2016).

⁸⁶⁰ James R. Liddle, Lance S. Bush, and Todd K. Shackelford, "An Introduction to Evolutionary Psychology and Its Application to Suicide Terrorism", *Behavioral Sciences of Terrorism and Political Aggression* 3, (2011): 176–197.

Sexual Offending as a Weapon of Terror

Armed conflict is considered one of the most reliable contexts predicting the perpetration of rape⁸⁶¹. Warfare is accompanied by sufficiently low risks for perpetrators, anonymity and/or impunity from repercussions, and high vulnerability of victims – all conditions that favor rape perpetration⁸⁶². Terrorists often consider themselves “at war” with a larger power⁸⁶³, such as a nation state, and so it follows that insofar as sexual offense are characteristic of periods of war, they also may become characteristic of terrorist activity (although it should be noted that how terrorists regard themselves is different from how governments regard terrorist activity, as crime and/or act of war⁸⁶⁴). Terrorist organizations are rarely in a position to make use of widespread sexual offending such as during war. However, some recent examples of terrorist organizations successfully engaging in open conflict demonstrate how sexual offenses may be incorporated into strategies to induce terror under certain conducive circumstances.

The atrocities of the so-called Islamic State (ISIL; the present analysis will follow the naming convention of the United States Department of State Bureau of Counterterrorism⁸⁶⁵ here and throughout, while acknowledging that there is considerable controversy regarding the naming of Islamic State^{866, 867}) in Iraq and Syria, beginning in 2013, brought international attention to the use of sexual offenses by terrorists. ISIL has employed sexual offenses

⁸⁶¹ Thornhill and Palmer, *A Natural History of Rape*.

⁸⁶² Jonathan Gottschall, “Explaining Wartime Rape”, *The Journal of Sex Research* 41, (May 2004), 129–136.

⁸⁶³ Bruce Hoffman, *Inside Terrorism*, 21–24.

⁸⁶⁴ Andrew Majoran, “The Illusion of War: Is Terrorism A Criminal Act or an Act of War?” *The Mackenzie Institute*, August 1, 2014, <https://mackenzieinstitute.com/2014/08/the-illusion-of-war-is-terrorism-a-criminal-act-or-an-act-of-war/>.

⁸⁶⁵ “Foreign Terrorist Organizations”, U.S. Department of State Bureau of Counterterrorism, accessed November 19, 2020, <https://www.state.gov/foreign-terrorist-organizations/>.

⁸⁶⁶ Taylor Wofford, “ISIL, ISIS or IS? The Etymology of the Islamic State”, *Newsweek*, September 16, 2014, <https://www.newsweek.com/etymology-islamic-state-270752>.

⁸⁶⁷ George Petras, “‘Daesh,’ Other Islamic State Names Explained”, *USA Today*, November, 17, 2015, <https://www.usatoday.com/story/news/world/2015/11/17/islamic-state-names/75889934/>.

widely, sometimes to directly intimidate groups that it considers a threat to its ideology⁸⁶⁸. Although morally objectionable, the integration of sexual offending into ISIL's strategy of inducing fear can be considered successful. Many refugees from the ISIL conflict reported fear of rape as one of the motivations for fleeing the group⁸⁶⁹. Media coverage of the sexual offenses of ISIL has been widespread. In addition, ISIL has been prolific in its use of social media, even advertising its sexual offenses via the internet⁸⁷⁰. Broadcasting its crimes, including sexual offenses, has been key to its ability to spread terror and remove local resistance through intimidation.

ISIL is not the only terrorist organization to have prominently spread terror through sexual offenses. For many people outside of west Africa, the first introduction to Boko Haram⁸⁷¹ (see above note for naming conventions) came with the organization's abduction of over 200 school-aged girls in April 2014 in Chibok, Nigeria⁸⁷². The ensuing widespread coverage in major Western media outlets unleashed a torrent of passionate, albeit faddish and impotent, social media condemnation against this attack⁸⁷³. However heinous that attack was, it is only a fraction of Boko Haram's sexual offenses. Boko Haram terrorists have extensively used the threat of forced marriage, sexual slavery, and rape to punish or prevent through terror, behaviours prohibited by its ideology (such as participating in non-Islamic education), according to witnesses and survivors⁸⁷⁴. In addition, Boko Haram terrorists have pursued sexual offenses for the purpose of impregnating

⁸⁶⁸ Malik, "Trafficking Terror", 17–18.

⁸⁶⁹ The Associated Press, "Iraqis Fleeing ISIS Militants Reveal Fears of Rape, Kidnapping", *NBC News*, June, 13, 2014, <https://www.nbcnews.com/storyline/iraq-turmoil/iraqis-fleeing-isis-militants-reveal-fears-rape-kidnapping-n130281>.

⁸⁷⁰ Rukmini Callimachi, "ISIS Enshrines a Theology of Rape", *New York Times*, August 13, 2015, https://www.nytimes.com/2015/08/14/world/middleeast/isis-enshrines-a-theology-of-rape.html?_r=2.

⁸⁷¹ "Foreign Terrorist Organizations", Bureau of Counterterrorism, <https://www.state.gov/foreign-terrorist-organizations/>.

⁸⁷² Aminu Abubakar, "As Many as 200 Girls Abducted by Boko Haram, Nigerian Officials Say", *CNN*, April 16, 2014, <https://www.cnn.com/2014/04/15/world/africa/nigeria-girls-abducted/index.html>.

⁸⁷³ Maeve Shearlaw, "Did the #bringbackourgirls Campaign Make a Difference in Nigeria?" *The Guardian*, April 14, 2015, <https://www.theguardian.com/world/2015/apr/14/nigeria-bringbackour-girls-campaign-one-year-on>.

⁸⁷⁴ Charlotte Alter, "Girls Who Escaped Boko Haram Tell of Horrors in Captivity", *Time*, October 27, 2014, <https://time.com/3540263/girls-boko-haram-escape/>.

women in order to breed a new generation of terrorists⁸⁷⁵. To this end, the terrorist organization is using sexual offenses not only to spread fear, but also for a strategic aim – increasing manpower and ensuring the continuity of the group across generations through its members’ pursuit of a facultative mating strategy⁸⁷⁶.

ISIL and Boko Haram are only two examples of how sexual offenses can become part of terrorist activities to spread terror. The conditions in which these groups have operated feature relatively weak or ineffective legal and security structures from the state, meaning the members of these organizations have been able to sexually offend at a far wider scale than is possible for many other terrorist organizations. This conclusion does not imply that other terrorists have not, do not, and will not commit sexual offenses to further their strategic goals; only that ISIL and Boko Haram have been able to perpetrate such offenses with uncommonly high frequency relative to other terrorists. Because of the scale of perpetration, sexual offenses have reasonably instilled fear of these organizations.

Sexual Offending as a Recruiting Tool

Although there are noted instances of women engaging in terrorist activity and even founding terrorist organizations (e.g., the Weatherman and the May 19th Communist Organization in the United States⁸⁷⁷, Gudrun Enslin and the Red Army Faction in Germany,⁸⁷⁸ and female Islamist suicide bombers⁸⁷⁹), most terrorists are men⁸⁸⁰. This effect follows the larger pattern of aggression in humans – men are primarily the perpetrators (and

⁸⁷⁵ Malik, “Trafficking in Terror”, 31–32.

⁸⁷⁶ William F. McKibbin et al., “Why Do Men Rape? An Evolutionary Psychological Perspective”, 90.

⁸⁷⁷ William Rosenau, “The Dark History of America’s First Female Terrorist Group”, *Politico*, May 3, 2020, <https://www.politico.com/news/magazine/2020/05/03/us-history-first-women-terrorist-group-191037>.

⁸⁷⁸ Maniszewska, *Pionierzy Terroryzmu Europejskiego*, 34.

⁸⁷⁹ Elizabeth Nolen, “Female Suicide Bombers: Coerced or Committed?” *Global Security Studies* 7, (Spring 2016): 30–40.

⁸⁸⁰ Jessica Trisko Darden, *Tackling Terrorists’ Exploitation of Youth*, American Enterprise Institute, 2019, 6. <https://www.aei.org/wp-content/uploads/2019/05/Tackling-Terrorists-Exploitation-of-Youth.pdf>.

targets) of aggression^{881, 882, 883}. The same pattern of behaviour is true of organized aggression. The formation of coalitions for warfare has been an exclusively male-initiated endeavor across human history⁸⁸⁴. In fact, in no culture have women been observed regularly forming coalitions designed to attack and kill conspecifics (see Buss, 2019 for a review⁸⁸⁵). These sex differences are the result of selection pressures that have favored the evolution of aggression as a solution to adaptive problems faced more often by males than by females. Indeed, men appear to be designed for intra-sexual competition, including the use of aggression⁸⁸⁶. Throughout human evolutionary history, coalitional warfare has been a route for victors to gain resources, including and especially mates (see Savage and Palmer, 2016⁸⁸⁷ for a review), which would have been a more salient problem for ancestral men compared to ancestral women. To that end, insofar as any armed conflict – be it a formal war between nation states, a turf war between rival street gangs, or terrorism – is predominantly the enterprise of men, it can be considered the result of an evolutionary history that has selected a propensity for aggression in men as a means of solving problems related to survival and reproduction^{888, 889, 890}. Therefore, it is not surprising that

⁸⁸¹ John Archer, "Sex Differences in Aggression in Real-World Settings: A Meta-Analytic Review", *Review of General Psychology* 8, (2004): 291–322.

⁸⁸² Martin Daly and Margot Wilson, *Homicide* (Hawthorne, NY: Aldine, 1988), 149.

⁸⁸³ Janet Hyde, "Gender Differences in Aggression", in *The Psychology of Gender: Advances through Meta-analysis*, eds. J.S. Hyde & M.C. Linn (Baltimore: Johns Hopkins University Press, 1986), 67–101.

⁸⁸⁴ Melissa M. McDonald, Carlos D. Navarrete, and Mark Van Vugt, "Evolution and the Psychology of Intergroup Conflict: The Male Warrior Hypothesis". *Philosophical Transactions of the Royal Society B: Biological Sciences* 367, (2012): 671–673.

⁸⁸⁵ Buss, *Evolutionary Psychology*, 289–297.

⁸⁸⁶ McDonald, Navarrete, and Van Vugt, "Evolution and the Psychology of Intergroup Conflict", 670–679.

⁸⁸⁷ Chet R. Savage and Craig T. Palmer, "Sexual Access as a Benefit of War", in *Encyclopedia of Evolutionary Psychological Science*, ed. Todd K. Shackelford and Viviana A. Weekes-Shackelford (Springer, Cham, 2016).

⁸⁸⁸ John Archer, "Does Sexual Selection Explain Human Sex Differences in Aggression?" *Behavioral and Brain Sciences* 32, (2009): 249–311.

⁸⁸⁹ McDonald, Navarrete, and Van Vug "Evolution and the Psychology of Intergroup Conflict", 670–679.

⁸⁹⁰ Robert L. Trivers, "Parental Investment and Sexual Selection", in *Sexual Selection and the Descent of Man 1871–1971*, ed. Bernard Campbell (Chicago: Adaline, 1972), 136–179.

sexual access, including through offending, can entice individuals (men) to join terrorist organizations.

ISIL again demonstrates a powerful example of how sexual offenses can impact recruitment to terrorist organizations. Women and girls captured by ISIL in Iraq and Syria were⁸⁹¹ often subject to rape and sexual slavery at the hands of their captors. The genocide of the ethno-religious minority Yazidi community in Iraq highlights the frequency of sexual offending by ISIL terrorists⁸⁹² and its effectiveness for drawing individuals into the group. Western media outlets have reported innumerable accounts of forced marriages, including the outright purchase of captured women and girls by ISIL terrorists as “spoils of war”⁸⁹³. These captives became a powerful currency for the terrorists, and a means of drawing the attention of perspective members. Although demographic data are incomplete, the average age of ISIL terrorists between 2013–2014 (around the height of the organization’s influence) was estimated to be about 26 years⁸⁹⁴. Male intrasexual competition (including for resources and mates) is most intense during teenage years and through young adulthood⁸⁹⁵, so it is not surprising that ISIL’s promise of wives could appeal to some young men (although other motivations are not discounted). It has also been suggested that men with a history of sexual violence may be differentially drawn to joining terrorist organizations⁸⁹⁶, although the idea of past sexual offending as a predictor of terrorist activities needs further empiri-

⁸⁹¹ ISIL will be referenced in the past tense here in recognition of the decline and hopeful dissolution of the group. However, at the time of writing, ISIL is still an active terrorist organization.

⁸⁹² Samar El-Masri, “Prosecuting ISIS for the sexual slavery of the Yazidi women and girls”, *The International Journal of Human Rights* 22, (2018): 1047–1066.

⁸⁹³ Annabell Van den Berghe, “Humiliation replaces fear for the women kidnapped by Isis”, *The Guardian*, October, 19, 2014, <https://www.theguardian.com/world/2014/oct/19/isis-forced-marriage-syria-iraq-women-kidnapped>.

⁸⁹⁴ Jack Moore, “New Analysis Shows ISIS Fighters Originate From 70 Countries”, *Newsweek*, April 20, 2016, <https://www.newsweek.com/new-analysis-shows-isis-fighters-originate-70-countries-449968>.

⁸⁹⁵ Margo Wilson and Martin Daly, “Competitiveness, Risk Taking, and Violence: The Young Male Syndrome”, *Ethology and Sociobiology* 6, 59–73.

⁸⁹⁶ Izzy Ferris, “Men with Histories of Sexual Violence are ‘More Likely to Be Terrorists’ so Police Should Monitor Them, Top Lawyer Claims”, *Daily Mail*, May 26, 2019, <https://www.dailymail.co.uk/news/article-7073493/Men-histories-sexual-violence-likely-terrorists-lawyer-claims.html>.

cal research (see Conclusions and Further Directions). However, at least some captured ISIL terrorists have admitted their willing participation in countless rapes⁸⁹⁷.

Forced marriages and sexual slavery of captured women and girls are not the only means by which ISIL was able to capitalize on sexual opportunities as a recruiting tool. It is estimated that thousands of women from outside of Iraq and Syria immigrated to areas under ISIL control to join the organization⁸⁹⁸. Although many of these women voluntarily married and bore children of ISIL terrorists, some may still be considered victims of sexual exploitation because of deceptive tactics used to lure them, and coercion and aggression used to entrap them in their marriages⁸⁹⁹. Entrapping willing women into involvement with the organization provides “rewards” for current members, but also an additional source of opportunity to recruit other members. The promise of reproductive opportunities is a powerful motivator for men to join armed coalitions. Where terrorist organizations can make believable promises of access to mates, they can increase their ability to recruit new members. One such avenue to make these promises credible is by sexual offending.

Financing Terrorism

Like many illicit activities, sexual offending can carry economic benefits for terrorist organizations. The clearest example of financial gain through sexual offending is the trafficking in persons for prostitution and other sex work. Human trafficking (the present analysis will use the terms “human trafficking” and “trafficking in persons” interchangeably, following

⁸⁹⁷ Michael Georgy, “Captive Islamic State Militant Says Mass Rapes Were ‘Normal’,” *Reuters*, February 17, 2017, <https://www.reuters.com/article/us-mideast-crisis-mosul-prisoners-idUSKBN15W1N0>.

⁸⁹⁸ Joana Cook and Gina Vale, *From Daesh to ‘Diaspora’: Tracing the Women and Minors of Islamic State* (London: International Centre for the Study of Radicalisation 2018) 3. https://icsr.info/wp-content/uploads/2018/07/Women-in-ISIS-report_20180719_web.pdf.

⁸⁹⁹ Ashley Binetti, “A New Frontier: Human Trafficking and ISIS’s Recruitment of Women from the West,” Georgetown Institute for Women, Peace and Security: 2015. <https://giwps.georgetown.edu/wp-content/uploads/2017/10/Human-Trafficking-and-ISISs-Recruitment-of-Women-from-the-West.pdf>.

the definition of U.S. Department of State⁹⁰⁰) is a lucrative and growing criminal business venture⁹⁰¹, and this financial potential is not without notice by terrorists. “For profit” criminal organizations have established a model for how to monetize sexual offending⁹⁰², and the distinction between (non-terrorist) criminal organizations and (criminal) terrorist organizations is becoming increasingly blurred when it comes to profiting from human trafficking⁹⁰³. It is possible that shared business interests may be producing closer ties and even formal cooperation between terrorist groups and criminal networks⁹⁰⁴. Prostitution provides a relatively easy and steady flow of money after initial investments are made⁹⁰⁵. Because it is illegal in the vast majority of jurisdictions, prostitution is often controlled by parties who attempt to operate beyond state regulation and oversight. As such, the proceeds from this contraband economy are also unregulated, and can be channelled into other illegal activities, such as terrorism. Human trafficking for prostitution and other sex work can be conducted at a variety of levels, from small local groups, to transnational organizations,⁹⁰⁶ meaning even terrorist organizations with modest global footprint can profit from it.

Financial opportunities from sexual offenses are not limited to prostitution. Although some terrorist organizations may have theoretical objections to its consumption, pornography carries tremendous financial potential. Profiting from pornography would mirror other underground enterprises already used by some terrorist organizations, such as narcotics

⁹⁰⁰ “Human Trafficking”, U.S. Department of State, accessed November 22, 2020, <https://www.state.gov/policy-issues/human-trafficking/>.

⁹⁰¹ United Nations Office on Drugs and Crime, *Global Report on Trafficking in Persons 2018* (Vienna: United Nations, 2018), https://www.unodc.org/documents/data-and-analysis/glotip/2018/GLOTIP_2018_BOOK_web_small.pdf.

⁹⁰² Steward Harrison Oppong, “Human Trafficking through Organized Crime”, *International Journal of Humanities and Social Science* 2, (October 2012): 37–43.

⁹⁰³ Counter-Terrorism Committee Executive Directorate, *Identifying and Exploring the Nexus between Human Trafficking, Terrorism, and Terrorism Financing*.

⁹⁰⁴ Nikita Malik, “Trafficking Terror”, 46–47.

⁹⁰⁵ DiGiacomo, “Prostitution as a Possible Funding Mechanism for Terrorism”, 22, 39.

⁹⁰⁶ Counter-Terrorism Committee Executive Directorate, *Identifying and Exploring the Nexus between Human Trafficking, Terrorism, and Terrorism Financing*.

trafficking⁹⁰⁷, counterfeiting and pirating, and extortion and kidnaping⁹⁰⁸. Revenues from the pornography industry are notoriously difficult to estimate, in part because some of the largest producers are privately held companies which do not release their financial information. However, it has been estimated that the pornography industry generates tens of billions of U.S. dollars annually in the United States alone⁹⁰⁹. To the author's knowledge, no open-source data yet link terrorist organizations to the sale or distribution of pornography, but with such high economic stakes, it seems likely that terrorist organizations may attempt to branch into this industry, if they have not already. Pornography can be a legitimate business venture, but it can also be used in concert with other sexual offenses, such as human trafficking. Individuals who are trafficked for prostitution could be trafficked similarly to create sellable pornographic content, making pornography an additive source of income. Children may be especially vulnerable for pornographic exploitation, because child pornography caters to a niche demographic with no legal business competition. Further, some terrorist organizations may not even have theoretical objections to such content, as demonstrated by ISIL posting recommendations condoning the rape of prepubescent captives via Twitter⁹¹⁰. Terrorist organizations have already demonstrated a willingness to compromise or morph their own ideological beliefs for profit (such as the Taliban's trade in opium and heroin⁹¹¹), so it would be unreasonable to rule out the possibility of involvement in the sale and distribution of pornography. Further, many terrorist organizations have demonstrated a keen use of the internet for propaganda and financing⁹¹², so they have the technical capacity to engage in

⁹⁰⁷ Colin P. Clarke, "Drugs & Thugs: Funding Terrorism through Narcotics Trafficking", *Journal of Strategic Security* 9, (Fall 2016): 1–15.

⁹⁰⁸ Michael Freeman, "The Sources of Terrorist Financing: Theory and Typology", *Studies in Conflict & Terrorism* 34, (2011): 461–475.

⁹⁰⁹ Ross Benes, "Porn Could Have a Bigger Economic Influence on the US than Netflix", *YahooFinance*, June 20, 2018, <https://finance.yahoo.com/news/porn-could-bigger-economic-influence-121524565.html>.

⁹¹⁰ Callimachi, "ISIS Enshrines a Theology of Rape".

⁹¹¹ David Mansfield, "Denying Revenue or Wasting Money? Assessing the Impact of the Air Campaign Against 'Drugs Labs' in Afghanistan", London: London School of Economics and Political Science, April 2019, 6–8. <https://www.lse.ac.uk/united-states/Assets/Documents/mansfield-april-update.pdf>.

⁹¹² Michael Jacobson, "Terrorist Financing and the Internet", *Studies in Conflict & Terrorism* 33, (2010): 353–363.

the trade of internet pornography. Profit from pornography need not be limited to sales. Documentation of sexually explicit content (either consensual or nonconsensual), such as videos, can be leveraged for blackmail or extortion, a term called “sextortion”⁹¹³. For instance, a terrorist could create or otherwise obtain (such a through hacking) a sexually explicit video of an individual and threaten to distribute it online if he does not receive a monetary payment. The use of sexploitation for profit is growing among individual and organized criminals⁹¹⁴, and is a relatively gainful enterprise. Because of the ease of production and distribution, and the potential profitability, it will be prudent for scientists and security professionals to monitor the use of pornography among other sexual offenses for fundraising by terrorists in the future.

Conclusion and Future Directions

There can be no doubt that committing sexual offenses has the potential to advance the strategic interests of terrorist organizations. Sexual offenses may be implemented to spread terror alongside other forms of aggression and violence. Terrorists may also use sexual offenses to recruit new members and finance their operations. It is becoming ever apparent that terrorists have the potential to become among the most widespread and organized perpetrators of sexual offenses. Because sexual offenses can cause grave harm to victims, as well as great benefits to terrorists, policy makers and security officials will need to continue global efforts to combat sexual offending in all forms. In order for preventative policies to be enacted and executed, officials must be armed with valid and reliable empirical data. Policies are only as effective as the research upon which they are built. Similarly, tactics and procedures to enact policies should be informed and improved by empirical research. As such, the burden falls to scientists to continue to collect new data, and synthesize existing data on the topics of sexual offending and terrorism, and to package and publish

⁹¹³ Roberta Liggett O’Malley and Karen M. Holt, “Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime”, *Journal of Interpersonal Violence* online first, (2020): 1–26, <https://doi-org.huayu.kl.oakland.edu/10.1177/0886260520909186>.

⁹¹⁴ Roberta Liggett, “Exploring Online Sextortion”, *Family & Intimate Partner Violent Quarterly* 11, (2019): 45–56.

these results into workable, consumable scientific theories that can influence tangible efforts to prevent these violations of human rights.

The role of the internet as a medium for criminal and terrorist activities bears particular attention with regard to sexual offending. Internet platforms allow terrorists to efficiently and quickly propagate news and threats of sexual crimes in order to intimate adversaries. Such broadcasting can also be an effective means of reaching and radicalizing new recruits to their causes, especially when sexual opportunities are being advertised as a reward to young men for joining. The internet has also created a new marketplace where both real and cryptocurrency can be easily collected in payment for sexual offenses, such as the purchase of persons. Therefore, researchers investigating terrorism and media⁹¹⁵ will need to consider sexual offending as a major terrorist activity that is easily facilitated by the use of information technologies such as the internet.

Although the present analysis has focused primarily on the macroscopic level of sexual offending by terrorist organizations, it is important to recognize that such organizations are made up of individual terrorists. Studying terrorist organizations is complementary to studying predictors of individual perpetration of sexual offenses, by terrorists and non-terrorists alike. Just as specific risk factors for joining terrorist organizations are being investigated^{916, 917}, so too must scientists examine how these factors may interact with the perpetration of sexual offenses. One such important research question is the extent to which men with a history or propensity for sexual offending may or may not be particularly susceptible to radicalization or joining terrorist organizations. This question intersects with the larger body of research on variables that predict sexual offending in general⁹¹⁸. Although there have been many programs that have reduced sexual

⁹¹⁵ Maura Conway, "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research", *Studies in Conflict & Terrorism* 40, (2017): 77–98.

⁹¹⁶ Arie W. Kruglanski and Shira Fishman, "Terrorism between Syndrome and Tool", *Current Directions in Psychological Science* 15, (2006): 45–48.

⁹¹⁷ Randy Borum, "Assessing Risk for Terrorism Involvement", *Journal of Threat Assessment and Management* 2, (2015): 63–87.

⁹¹⁸ Martin L. Lalumière et al., *The Causes of Rape*.

offending, it remains disturbingly recurrent, thus suggesting that efforts to reduce sexual offending are based on an inadequate understanding of the component phenomena. Research on sexual offending must integrate variables at every level of analysis of proximate causes (including individual differences, groups, and larger social structures^{919, 920}) as well as ultimate causes (derived from Tinbergen's [1963] famous four questions⁹²¹). To prevent sexual offending by individual terrorists and organizations, a comprehensive scientific theory is needed. Such a theory must coalesce research on individual differences (e.g., genetics, neurological function and structure, psychological mechanisms), social and cultural mechanisms (e.g., situations likely to produce sexual offenses, group pressure, cultural expectations of permissible sexual activity), and explanations about human evolved psychology (e.g., men's disposition towards aggression, rape as an adaptation), as well as collect new data on these variables in order to understand sexual offending. Only once this scientific theory is adequately supported by empirical data will efforts to combat sexual offending have acceptably high efficacy. Doing so will be an enormous undertaking requiring unprecedented interdisciplinary collaboration, but because the consequences so high, this effort is more than justifiable, it is obligatory.

⁹¹⁹ Willem Doise and Joaquim Pires Valentin, "Levels of Analysis in Social Psychology", in *International Encyclopedia of the Social & Behavioral Sciences*, ed. James D. Wright (Oxford: Elsevier, 2015), 899–903. <https://doi.org/10.1016/B978-0-08-097086-8.24032-4>.

⁹²⁰ Neil M. Malamuth and Eldad Z. Malamuth, "Integrating Multiple Levels of Scientific Analysis and the Confluence Model of Sexual Coercers". *Jurimetrics* 39, (1999): 157–179.

⁹²¹ Niko Tinbergen, "On Aims and Methods of Ethology", *Zeitschrift für Tierpsychologie* 20, (1963): 410–433.

The Frequency and Influence of Far-Right Extremism in Current and Former American Military Personnel

Kathryn WESTON

Abstract: This paper examines the role of current and former American military personnel within white supremacist groups in the United States. I draw upon three specific case studies and broader FBI data to establish the influence and role of military personnel within white supremacist organizations. As this paper highlights, military personnel influence includes the contribution of skills acquired through specialized training in weapons, tactics, and organizational skills. The parameters of my research include three case studies from the past three years that effectively illustrate the reason for renewed interest in the issue. I will then explain the purpose and scope of an assessment conducted by the Department of Homeland Security Office of Intelligence and Analysis and the consequent public outrage after its leak; following this, I will summarize the findings in an FBI assessment on military recruits in white supremacist organizations in the United States. Finally, I will propose my own solutions, which include renewing the government's research efforts to accommodate online participation in this movement.

Keywords: far-right, white supremacy, Atomwaffen, Boogaloo, United States military, FBI, DHS

Introduction

Since 2016, there has been renewed interest of far-right movements in the USA following a series of recent events – the rise of the alt-right online movement during the 2016 presidential election cycle, the white supremacist rally in Charlottesville, North Carolina in 2017, a rally of various far-right groups that gathered in protest against the removal of the Robert E. Lee statue in Charlottesville, and a violent clash between protesters and counter protesters that led to the death of a young woman⁹²².

With the evolving landscape in the far-right movement, this paper seeks to understand the role military personnel have played. To answer this questions, this paper examines three recent cases whereby military personnel were involved and arrested for far-right extremist activity. However, before proceeding to these case studies, it is important to underline that it is not the intention of this paper to mischaracterize American military personnel, veterans, and persons involved in politically conservative activism. As this paper points out, the number of current and former American service members active in far-right extremist groups is relatively low. Between October 2001 and May 2008 for example, the FBI identified 203 cases active in the white supremacist extremist movement among an active duty military personnel and veteran population of 25,232,037⁹²³. Furthermore, there are cases of persons in the military with extremist ideologies other than far-right. An example is American Army Major Nidal Hassan, responsible for the massacre at Fort Hood in 2009. Hassan had been in contact with an al-Qaeda propagandist before the attack⁹²⁴. Finally, there have also been cases of military personnel be-

⁹²² Jacey Fortin, “The Statue at the Center of Charlottesville’s Storm”, The New York Times, Published 13 August 2017; accessed 17 August 2020, <https://www.nytimes.com/2017/08/13/us/charlottesville-rally-protest-statue.html>.

⁹²³ FBI Counterterrorism Division, *White Supremacist Recruitment of Military Personnel since 9/11*, Published 7 July 2008; accessed 10 August 2020, <https://documents.law.yale.edu/sites/default/files/White%20Supremacist%20Recruitment%20of%20Military%20Personnel%20Since%209-11-ocr.pdf>, 5.

⁹²⁴ Kyle Rempfer, “The mass shooting at Fort Hood was 10 years ago, on Nov. 5, 2009”, Army Times, Published 5 November 2019; accessed 18 August 2020 <https://www.armytimes.com/news/your-army/2019/11/05/the-mass-shooting-at-fort-hood-was-10-years-ago-on-nov-5-2009/>.

ing targeted, and sometimes killed, by extremists; however, there were no fatalities of military personnel by far-right extremists from 1990–2015, all U.S. military victims of extremism from the period were killed in acts of Islamist extremism⁹²⁵.

With these considerations and clarification in mind, I will now proceed to three recent case studies that illustrate the role of military personnel within current far-right movements.

Recent Case Studies

Atomwaffen Division in Florida

In May 2017, police in Tampa, Florida, questioned two suspects after the murder of their roommate. The three young men were members of the Atomwaffen Division, a white supremacist organization determined to ignite a race war. While one of the men confessed to the murder, Brandon Russell was released after questioning; within hours, Russell, a member of the Florida Army National Guard, was pulled over by police for transporting weapons and ammunition. The authorities suspected that Russell and another Atomwaffen member were going to commit a mass shooting⁹²⁶.

Boogaloo in Las Vegas

Three men with military experience were arrested and charged on 30 May 2020 with “violations of federal and state law for conspiracy to cause destruction during protests in Las Vegas, and possession of an unregistered

⁹²⁵ William Parkin, Brent Klein, Jeff Gruenewald, Joshua Freilich, and Steven Chermak, “Threats of violent Islamist and far-right extremism: What does the research say?” National Consortium for the Study of Terrorism and Responses to Terrorism, Published 17 February 2017; accessed 17 August 2020, <https://www.start.umd.edu/news/threats-violent-islamist-and-far-right-extremism-what-does-research-say>.

⁹²⁶ A.C. Thompson, “An Atomwaffen Member Sketched a Map to Take the Neo-Nazis Down. What Path Officials Took Is a Mystery”, Pro Publica, Published 20 November 2018; accessed 24 September 2020, <https://www.propublica.org/article/an-atomwaffen-member-sketched-a-map-to-take-the-neo-nazis-down-what-path-officials-took-is-a-mystery>.

destructive device.”⁹²⁷. These men were allegedly active in the Boogaloo movement, an amorphous and factious movement whose broad beliefs include an immanent American civil war⁹²⁸. The men were seeking to take advantage of the protests expressing outrage over the death of George Floyd, a black man who was killed after a police officer pressed his knee against Floyd’s neck for several minutes; the men allegedly wished to use the protests to further their own anti-police and anti-government agendas.

Stephen T. Parshall, 35, was formerly enlisted in the Navy; Andrew T. Lynam Jr., 23, is an Army reservist; and William L. Loomis, 40, was formerly enlisted in the Air Force⁹²⁹.

Boogaloo in California

Steven Carrillo, 32, a sergeant in the Air Force, was charged with murder and attempted murder after allegedly killing a federal security guard and wounding his partner during protests against police brutality on 29 May 2020. A week later, he allegedly killed a police officer and wounded a second after a concerned resident reported seeing stockpiled weapons on Carrillo’s property. Carrillo had recently posted memes on Facebook favorable to the Boogaloo movement⁹³⁰.

⁹²⁷ Department of Justice, “Joint Terrorism Task Force Charges Three Men Who Allegedly Sought To Exploit Protests In Las Vegas And Incite Violence”, U.S. Attorney’s Office, District of Nevada, Published 3 June 2020; accessed 16 August 2020, <https://www.justice.gov/usao-nv/pr/joint-terrorism-task-force-charges-three-men-who-allegedly-sought-exploit-protests-las>.

⁹²⁸ Robert Evans and Jason Wilson, “The Boogaloo Movement Is Not What You Think”, Bellingcat, Published 27 May 2020; accessed 16 August 2020, <https://www.bellingcat.com/news/2020/05/27/the-boogaloo-movement-is-not-what-you-think/>.

⁹²⁹ Michelle L. Price and Scott Sonner, “Army reservist, Navy and Air Force vets plotted to terrorize Vegas protests, prosecutors charge”, Military Times, Published 4 June 2020; accessed 16 August 2020, <https://www.militarytimes.com/news/your-military/2020/06/04/army-reservist-navy-and-air-force-vets-plotted-to-terrorize-vegas-protests-prosecutors-charge/>.

⁹³⁰ Nate Gartrell and Fiona Kelliher, “Santa Cruz deputy’s alleged killer charged with assassinating federal cop in Oakland ambush; authorities link attacks to extremist group that believes civil war looming”, Santa Cruz Sentinel, Published 16 June 2020; accessed 17 August 2020, <https://www.santacruzsentinel.com/2020/06/16/santa-cruz-deputys-alleged-killer-charged-with-assassinating-federal-cop-in-oakland-ambush/>.

The DHS Assessment

On 14 April, 2009, a copy of an assessment by the Department of Homeland Security (DHS) Office of Intelligence and Analysis, titled “Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment” was leaked to the media⁹³¹. The scope and purpose of this assessment, as stated in the text, is “to facilitate a greater understanding of the phenomenon of violent radicalization in the United States.”⁹³² It cites the prevailing economic and political climate, the election of the country’s first Black president, illegal immigration, possible new gun restrictions, and the challenges of returning veterans as factors that contribute to a fertile ground for rightwing radicalization⁹³³. The assessment defines rightwing extremism as follows:

“Rightwing extremism in the United States can be broadly divided into those groups, movements, and adherents that are primarily hate-oriented (based on hatred of particular religious, racial, or ethnic groups), and those that are mainly antigovernment, rejecting federal authority in favor of state or local authority, or rejecting government authority entirely. It may include groups and individuals that are dedicated to a single issue, *such as opposition to abortion*⁹³⁴ or immigration”⁹³⁵.

The assessment goes on to describe the American militia movement of the 1990s and the political themes therein. The purpose of the section is to draw a parallel from the national climate of the previous decade to the prevailing national climate at the time of the assessment; such political themes include criticism of free trade agreements and the white

⁹³¹ U.S. Congress, House of Representatives, Committee on Homeland Security, *Resolution of Inquiry Regarding Department of Homeland Security Office of Intelligence and Analysis Intelligence Assessment Titled, “Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment”*, 111th Cong., 1st sess., 2009, H. Rep. 111–134, 3, congress.gov/congressional-report/111th-congress/house-report/134.

⁹³² U.S. Department of Homeland Security, “Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment”, Published 7 April 2009, 1.

⁹³³ DHS, 2.

⁹³⁴ Emphasis by author of the paper.

⁹³⁵ Ibid.

supremacists' exploitation of contentious social issues such as abortion and same-sex marriage⁹³⁶.

The assessment's focus on military veterans proved particularly controversial after the document's leak; moreover, conservative House members saw the document's mention of the opposition to free trade agreements, gun control, abortion, and same-sex marriage as distrust from the DHS towards persons with politically conservative values. As stated in House report 111–134, signed by the Republican Members of the Committee on Homeland Security, "The release of [the DHS] report raised serious concerns across the country about its depiction of military veterans as recruits for terrorists, as well as its overly broad characterizations of those who oppose gun control, free trade agreements, abortion, and same-sex marriage."⁹³⁷ The report required the Secretary to send all written documents and communications to the House for review⁹³⁸. The opprobrium also came from the public: David K. Rehbein, U.S. Army veteran and National Commander of The American Legion, wrote an open letter claiming that the DHS lacked statistical evidence in their assessment of returning military veterans⁹³⁹. Furthermore, characterizing Timothy McVeigh as the archetypal disillusioned military veteran is akin to characterizing Osama bin Laden as the typical Muslim⁹⁴⁰.

An assessment conducted by the FBI Counterterrorism Division was cited as a source in the DHS assessment⁹⁴¹. I will now summarize the FBI's findings on the participation of current and former military personnel in the white supremacist extremist movement.

⁹³⁶ DHS, 4.

⁹³⁷ U.S. Congress, House of Representatives, Committee on Homeland Security, *Resolution of Inquiry*, 3.

⁹³⁸ U.S. Congress, House of Representatives, Committee on Homeland Security, *Resolution of Inquiry*, 15.

⁹³⁹ David Rehbein, "An Open Letter to Homeland Security on 'Rightwing Extremists'", Fox News, Published 14 April 2009; accessed 10 August 2020, <https://www.foxnews.com/opinion/an-open-letter-to-homeland-security-on-rightwing-extremists>.

⁹⁴⁰ Ibid.

⁹⁴¹ DHS, 7.

The FBI Assessment

The purpose of the FBI's assessment⁹⁴², titled "White Supremacist Recruitment of Military Personnel since 9/11", is to examine the recruitment efforts of white supremacist organization toward current and former US military personnel⁹⁴³. The assessment's purpose is to determine the motivations of white supremacist groups in recruiting members with military experience, the successes of their recruitment efforts, and the impact of such recruitment on the white supremacist movement⁹⁴⁴.

The FBI identified 203 persons with "confirmed or claimed military service active in the extremist movement" between October 2001 to May 2008; this is out of a total 25,232,037 former and active military personnel in the time period⁹⁴⁵. The distribution across white supremacist extremist groups during this period is as follows⁹⁴⁶:

National Alliance	28%
Select Skinhead Groups	22%
National Socialist Movement	21%
Select Ku Klux Klan Groups	10%
Aryan Nations	8%
Creativity Movement	4%
Other	6%

⁹⁴² It is important to note that while the DHS assessment focuses on rightwing extremist groups broadly, the FBI report focuses on white supremacist groups specifically.

⁹⁴³ FBI Counterterrorism Division, *White Supremacist Recruitment of Military Personnel since 9/11*, Published 7 July 2008; accessed 10 August 2020, <https://documents.law.yale.edu/sites/default/files/White%20Supremacist%20Recruitment%20of%20Military%20Personnel%20Since%209-11-ocr.pdf>, 2.

⁹⁴⁴ Ibid.

⁹⁴⁵ FBI, 5.

⁹⁴⁶ Ibid.

Many of these groups made efforts to recruit candidates with military experience. William Luther Pierce, the founder of the National Alliance, sought to recruit “high quality”⁹⁴⁷ candidates from academia, law enforcement, and the military. In particular, he was interested in enrolling persons with military experience disgruntled by oversight from the United Nations.⁹⁴⁸ Moreover, the National Socialist Movement received inquiries from active military personnel stationed in Iraq and Afghanistan⁹⁴⁹. White supremacist skinhead leaders encouraged potential recruits lacking military experience to infiltrate the military to receive adequate training for the benefit of the movement⁹⁵⁰.

The statistics suggest the recruitment of and interest in military personnel joining alt-right groups is statistically low, however it should not be overlooked as it can pose a serious threat to security and enhance violent right wing extremist groups’ potential. Thus, I will now provide recommendations for how government institutions should move forward in addressing the issue.

Recommendations

Given the controversy the DHS report sparked, it is important that government agencies are careful in how they proceed with solutions. One must be sure to analyze the vulnerability of military personnel to extremism knowing that this issue can be politicized. Given the recent rise in white supremacist and far-right activity, however, it is likely that conservative politicians will give more consideration to information from the intelligence community on this matter.

There is an information gap regarding the path of radicalization of these military personnel. Questions that can guide further research include the

⁹⁴⁷ FBI, 6.

⁹⁴⁸ Ibid.

⁹⁴⁹ Ibid.

⁹⁵⁰ FBI, 7.

following: Is the subject sympathetic to a far-right cause preceding, during, or following their military service? If the person is radicalized before his enrollment in military service, then is weapons training a motivating factor in his enrollment? If he goes through radicalization during or following their military service, then does disillusionment and perceived lack of governmental support make him more vulnerable to extremist recruits? Identifying the various radicalization processes is key to preventing further radicalization in military personnel. This cannot be achieved, however, without thorough cooperation and introspection from the recovering extremists themselves.

Finally, further research is needed on the increased connectivity within the far-right global network; different far-right groups across the globe will continue to use efficient communication to further radicalize, recruit, and provide one another support. Increased monitoring across social media platforms and encrypted communications will further reveal the nature and overlap of intragroup connections across borders.

The Impact of Terrorism on Border Security in the EU: The Case of the Islamic State

Yasmeen JONES

Abstract: The Islamic State (IS) has been around since the 1990's under different leadership and commonly referred to as ISIS. It was not until 2013 when the group changed their name to the Islamic State. Since the 2000's, the expansion of the Islamic State has grown significantly. IS has been in battle to overtake many regions within Syria and Iraq to acquire control of lands and assets. US-led invasions with joint forces from Belgium, Denmark, France, Jordan, the Netherlands, and the UK have taken part of the coalition to deter and expel the rise of the Islamic State from gaining complete power in the Middle East. The economic advantages that IS receives from conquering different regions in Syria and Iraq comes with benefits such as oil, taxes, smuggling artifacts/art, and prospering from business deals with human trafficking dealers, which has given the terrorist organization the fundamental means to procure, govern, recruit, pay, and distribute their beliefs across the globe. The network of the terrorist organization has enlarged to a degree where there are individuals all over the world who pose a threat. Countries in the South/Southeast Asia (i.e. the Philippines) and in the EU (i.e. France, UK, Belgium, and Germany), have seen an increase in terrorist plots or attempted attacks within the past five years due to many Muslim citizens and non-Muslims citizens (i.e. young vulnerable males and criminals) being persuaded to convert into foreign fighters due to the progression of radicalization and digital recruiting methods used by IS. In response, the EU has enacted strict mandates formed for restrictions and more effect guidelines for border security, to deter any terrorist threat in the present and future times. Effective policies and border agencies such as FRONTEX and European Counter Terrorism Centre (ECTC) to challenge and mitigate any threat possible from entering into the EU. This paper analyzes the impact of terrorism organized and/or inspired by IS to EU security with a focus on border security.

Keywords: terrorism, IS, Islamic State

Introduction

“[T]errorism” Wardlaw argues, “may be aimed at causing/hastening a general breakdown in social order, demoralizing the citizens and causing them to lose faith in the ability of the incumbent government to maintain order, stability and safety.”⁹⁵¹

The Islamic State (IS) has been around since the 1990’s under different leadership and commonly referred to as ISIS, “Islamic State of Iraq, as al-Qaeda in Iraq (AQI), as Majlis Shura al Mujahidin, and as Jamaat al Tawhid wa-l-Jihad.”⁹⁵² This paper examines the IS and analyses the problems it has been causing the EU border security. In particular, this paper looks at how IS has been able to control many regions within Iraq and Syria, recruit new followers abroad called foreign fighters, obtain financial gains from oil, taxes, smuggling art/artifacts in the black-market, and affect the migration flow from certain countries.

As this paper highlights, IS has impacted individuals seeking refuge in European countries and discusses the EU response of increasing border security and agencies to control and counter any form of a terrorist threat/plot from affecting the security of its nations and its citizens. From 2014 to 2019, there have been numerous terrorist plots in the EU, with increases from 2015 to 2017 and a slight decrease from 2018 to 2019⁹⁵³. Examples of the types of terrorist plots include bombings such as (i.e. the bombing in Spain in 2004, terror attack in Strasbourg in 2018, the bombing in Brussels in 2016, and the Manchester Arena bombing in England in 2017”⁹⁵⁴). Due

⁹⁵¹ Grant Wardlaw, “Political Terrorism: Theory, tactics, and counter-measures”, Cambridge University Press, (1982): 39.

⁹⁵² Matthew Levitt, “Terrorist Financing and the Islamic State” Washington Institute for Near East Policy, November 13, 2014. Accessed July 31, 2020. <https://www.washingtoninstitute.org/uploads/Documents/testimony/LevittTestimony20141113.pdf>.

⁹⁵³ News – European Parliament, “Terrorism in the EU: terror attacks, deaths, and arrests in 2019”, July 14, 2020. Accessed date September 19, 2020, <https://www.europarl.europa.eu/news/en/headlines/security/20180703STO07125/terrorism-in-the-eu-terror-attacks-deaths-and-arrests-in-2019>.

⁹⁵⁴ Petter Nesser, “Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs” CTC Sentinel, May 2019. Accessed August 4, 2020. <https://ctc.usma.edu/wp-content/uploads/2019/03/CTC-SENTINEL-032019.pdf>

to the IS attacks in several European cities such as in Paris and Brussels, the terrorist organization has received world recognition for being an extremist Islamic group within a short time frame. Its ideologies have “made it a rival not only to western countries, but also to neighboring ones”⁹⁵⁵.

The Islamic State and Europe could be compared to a wildfire; that keeps burning, expanding, and reaching into more fields. The tensions between the two parties is one that may be lasting for a long time. The amount of water that is poured into the situation has not and will not dissipate until a solution is found and/ or the problem can be eliminated in all its entirety. EU and its allies versus IS are on a metaphorical battlefield of “tactical and strategic”⁹⁵⁶ elements. With IS on the rise, US-led coalitions along with countries such as France, UK, Belgium, and Germany have formed a team to fight against the insurgency of the Islamic State in “several African...and Middle Eastern countries such as Syria, Iraq, and Libya.”⁹⁵⁷ In order to stop the rise of the terrorist organization, the coalition to fight IS strikes where the organization gained the most support. The Islamic State has developed into a globally well-known terrorist organization and to some extent their own ‘state’. After taking control over several cities in Syria and Iraq, IS has acquired the “Administrative buildings, courts and street signs....military recruitment and financial means, social media outreach, and illegal operations”⁹⁵⁸, giving them the foundation to further build their caliphate.

Following IS overthrow of many cities in Iraq and Syria, the flow of migration has spiked in recent years. Over the course of the Syrian war, there has been an estimated 5.6 million Syrian refugees and another 6.2 million displaced within the country⁹⁵⁹. In 2015, Europe began to feel the pres-

⁹⁵⁵ Rafat Kurdi, “Islamic State” Listopad, (2016) https://www.amo.cz/wp-content/uploads/2016/11/NATO_isis_final.pdf.

⁹⁵⁶ Grant Wardlaw, “Political Terrorism: Theory, tactics, and counter-measures”, Cambridge University Press, (1982).

⁹⁵⁷ Rafat Kurdi, “Islamic State” Listopad, (2016) https://www.amo.cz/wp-content/uploads/2016/11/NATO_isis_final.pdf.

⁹⁵⁸ Rafat Kurdi, “Islamic State” Listopad, (2016) https://www.amo.cz/wp-content/uploads/2016/11/NATO_isis_final.pdf.

⁹⁵⁹ World Vision, “Syrian refugee crisis: facts, FAQ’s, and how to help”, March 15, 2020. Accessed August 7, 2020, <https://www.worldvision.org/refugees-news-stories/syrian-refugee-crisis-facts>.

sure of the influx of refugees and migrants when an estimated 1 million arrived looking for a better life and to flee from violence and war⁹⁶⁰. With the significant number of migrants and refugees coming into Europe, the EU has implemented various security measures in place for refugees and migrants in order to deter any potential threats that may come into European countries. In response to several violent conflicts and civil wars in the Middle East, joint coalitions between many countries in the EU and the US have developed to address the rise of radicalism and concerns of foreign fighters creating security obstacles within the EU borders.

In the years 2014 and 2015, the rise of the Islamic State and groups of similar ideologies have caused a prominent increase of 30,000 foreign fighters from over 100 UN Member States⁹⁶¹. How will this affect the EU? How will the security of the borders look since there is tension within the borders of people trying to cause/do harm and mayhem? Would a joint effective border security outline be promising? Are there future plans in place for an effective EU security strategy? This paper outlines the major threats IS is posing to EU security and measures the EU has taken to counter them, especially in the field of border security.

Islamic State of Iraq and Syria: Organization and Activity

Recruitment

Part of the Islamic State's strategy is to recruit and mobilize new members in the EU by means of entrepreneurs making contact and providing information about the terrorist organization. Entrepreneurs are in charge of "reaching out to misfits such as criminals and people who are socially distant and offer them a place of purpose and connection....and mold

⁹⁶⁰ World Vision, "Syrian refugee crisis: facts, FAQ's, and how to help", March 15, 2020. Accessed August 7, 2020, <https://www.worldvision.org/refugees-news-stories/syrian-refugee-crisis-facts>.

⁹⁶¹ Security Council Counter-Terrorism Committee of the United Nations, "Foreign terrorist fighters", 2014. Accessed September 19, 2020, <https://www.un.org/sc/ctc/focus-areas/foreign-terrorist-fighters/>.

them into terrorist.”⁹⁶² As Nesser discusses, these methods are effective and provide a sense of belonging to those normally deemed “misfits”⁹⁶³. Gates and Podder write how IS seeks to become global, with “Recruitment from parts of the world such as the Middle East, North Africa, and from Europe”⁹⁶⁴. IS also seeks to polarize “grayzones” – religiously mixed communities that might otherwise coexist peacefully. This is done by triggering hatred and retribution against Muslims in western countries. In 2015 for example, the Islamic State proclaimed that Muslims in the West have two choices – apostatize or emigrate to the Islamic State⁹⁶⁵. This proclamation came just prior to the massacre that IS incited in Paris of a satirical magazine named *Charlie Hebdo* promoting fear and heightening tensions between French Muslims and other French citizens.

GLOBSEC characterizes potential European Jihadis recruited as “male, young adults, homegrown and naturalized, unemployed, criminal, sometimes uneducated, slow to mature to radicalization, and traveling to and from a foreign conflict.”⁹⁶⁶ Foreign fighters with a criminal background typically have had “a serious run-in with the law....they had committed crimes including: violent robberies, burglaries, and thefts; illicit trafficking of drugs, trafficking of goods and fraud, and terrorism-related crimes.”⁹⁶⁷.

Propaganda is also used as part of the new recruitment strategy. Social media has been used as a media outlet for advertising and displaying what the Islamic State is about. The recruitment is not limited to any particular

⁹⁶² Petter Nesser, “Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs” CTC Sentinel, May 2019. Accessed August 4, 2020. <https://ctc.usma.edu/wp-content/uploads/2019/03/CTC-SENTINEL-032019.pdf>.

⁹⁶³ Petter Nesser, “Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs” CTC Sentinel, May 2019.

⁹⁶⁴ Scott Gates and Sukanya Podder, “Social Media, Recruitment, Allegiance and the Islamic State” Perspective on Terrorism, (2015): 107–113.

⁹⁶⁵ Murtaza Hussain, “Islamic State’s Goal: Eliminate the Grayzone”, The Intercept, November 15, 2015. Accessed August 5, 2020, <https://theintercept.com/2015/11/17/islamic-states-goal-eliminating-the-grayzone-of-coexistence-between-muslims-and-the-west/>.

⁹⁶⁶ GLOBSEC, “Who are the European Jihadis?” November 9, 2018. Accessed August 3, 2020. <https://www.globsec.org/publications/who-are-european-jihadis-from-criminals-to-terrorists-and-back/>.

⁹⁶⁷ GLOBSEC, “Who are the European Jihadis?” November 9, 2018. Accessed August 3, 2020. <https://www.globsec.org/publications/who-are-european-jihadis-from-criminals-to-terrorists-and-back/>.

person or set of skills⁹⁶⁸. With the advancement of the use of social media and any other forms of virtual propaganda, IS increases its chances of enlisting recruits with knowledge of “technical and machinery capabilities to help with the promotion and further spread the word. The virtual entrepreneurs are used to direct and recruit terrorist attacks in Europe and other places in the world via encrypted apps such as Telegram”⁹⁶⁹. This is how planned attacks are coordinated and planned through encrypted technology. Through such advanced forms of recruitment, IS has the ability to draw attention and attract new recruits to join.

To incite and motivate prospective new members, recruiters may include “the prospect of adventure, a search for identity, feeling of revenge, the desire to make history, the idea to die as a martyr and go to heaven in the end.”⁹⁷⁰. Common IS recruiter targets include Muslims, criminals, uneducated citizens, males, homegrown or naturalized citizens, and young adults⁹⁷¹. GLOBSEC reported that in 2015, “54% of incarcerated criminals later turned terrorist by co-radicalized behind bars in prison due to the contact of other radicalized prisoners”⁹⁷² who were caught doing terror-related crimes. Motivations to change their current lifestyle is an effective tool to further persuade someone to join the fight. This means traveling to another country to join the mission of such terrorist groups for training to be assimilated into the terrorist organization.

⁹⁶⁸ Scott Gates and Sukanya Podder, “Social Media, Recruitment, Allegiance and the Islamic State” (Perspective on Terrorism, 2015) 107–113.

⁹⁶⁹ Petter Nesser, “Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs” CTC Sentinel, May 2019. Accessed August 4, 2020. <https://ctc.usma.edu/wp-content/uploads/2019/03/CTC-SENTINEL-032019.pdf>.

⁹⁷⁰ Scott Gates and Sukanya Podder, “Social Media, Recruitment, Allegiance and the Islamic State” Perspective on Terrorism, (2015): 107–113.

⁹⁷¹ GLOBSEC, “Who are the European Jihadis?” November 9, 2018. Accessed August 3, 2020. <https://www.globsec.org/publications/who-are-european-jihadis-from-criminals-to-terrorists-and-back/>.

⁹⁷² GLOBSEC, “Who are the European Jihadis?” November 9, 2018. Accessed August 3, 2020. <https://www.globsec.org/publications/who-are-european-jihadis-from-criminals-to-terrorists-and-back/>.

Foreign Fighters

The mobilization of foreign fighters is influenced by the victimization or injustice done to civilians in a certain region from wars. Foreign fighters have mobilized and fought in past wars including the wars in Afghanistan, Bosnia, Chechnya, and Iraq. In the case of the recent war in Syria, IS has succeeded in attracting and recruiting a much larger pool of international foreign fighters in part because of the extensive international coverage it has received. The Islamic State has heavily relied upon the use of foreign fighters that have provided the terrorist organization with a diverse skills set that it would not have otherwise. Foreign fighters are defined as “non-citizens of conflict states who join insurgencies during civil conflicts.”⁹⁷³ With pressure at an all-time high between Europe and the Islamic State, there is no surprise that the recruitment of foreign fighters is heavy within countries with the highest rate of Muslim citizens and migration of Muslim refugees. Over the past 4 years between 2014–2018 there have been more terrorist plots in Europe. Nesser argues, “More people have died from terrorism in Europe between 2014 and 2018 at least 345 deaths than in the previous 20 years at 267 deaths.”⁹⁷⁴ As of March 2017, an estimated “40,000 individuals from 110 countries had traveled to Syria and/or Iraq to engage in combat as members for various armed groups since 2012”, many of which came from Europe⁹⁷⁵. The Islamic State seeks foreign fighters from the West to target countries with terrorist plots and attacks against countries who were part of the joint coalition against them. This strategy has succeeded in making IS one of the EU’s largest security threats, particularly in France and the UK, who have been the target of terrorist plots within the past years. Despite the UK and France’s promo-

⁹⁷³ David Malet, “Foreign fighters: Transnational identity in civil conflicts”. Oxford University Press, (2013).

⁹⁷⁴ Petter Nesser, “Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs” CTC Sentinel, May 2019. Accessed August 4, 2020. <https://ctc.usma.edu/wp-content/uploads/2019/03/CTC-SENTINEL-032019.pdf> page?

⁹⁷⁵ Christopher Blanchard and Carla Humud, “The Islamic State and U.S. Policy”, Congressional Research Service, September 25, 2018. Accessed August 11, 2020. <https://fas.org/sgp/crs/mideast/R43612.pdf>.

tion of multiculturalism⁹⁷⁶ or assimilation⁹⁷⁷ to integrate different religions, these two countries have faced the highest terrorist threats due to “their policies of intervening in armed conflicts in the Muslim world.”⁹⁷⁸

IS was able to exploit the migration crisis in 2015 by smuggling in terrorist plotters posing as refugees and by recruiting members among the refugees for attacks⁹⁷⁹. Also, they used routes via Istanbul to bring foreign fighters to Syria – they would “travel into northern Syria via Turkey by flying into Istanbul and transferring to commercial flight or buses to the border where they would either cross legally or smuggler routes.”⁹⁸⁰

The bridge between the Islamic State and Europe are the foreign fighters. Gates and Podder estimate “around 20 percent of foreign fighters who have traveled from western countries”⁹⁸¹ have joined conflicts in the Muslim world. Although many of the recruits from the West are inexperienced, Gates and Podder argue that they along with the other foreign fighters “can be trained to be excellent combatants, but most likely be given tasks unique to their skills.”⁹⁸²

In addition to European recruits, Gates and Podder reported that in 2015, “over 20,000 foreign fighters had joined militant organization in the Iraq/Syria conflict with most of them being Arabs coming from neighboring

⁹⁷⁶ Multiculturalism: the acknowledgement of a variety of cultures, races, and ethnicities of minority group differences within a dominant political culture. <https://www.britannica.com/topic/multiculturalism>.

⁹⁷⁷ Assimilation: the process difference of individuals or groups ethnic heritage are absorbed into the dominant culture of a society. <https://www.britannica.com/search?query=assimilation>.

⁹⁷⁸ Petter Nesser, “Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs” CTC Sentinel, May 2019. Accessed August 4, 2020. <https://ctc.usma.edu/wp-content/uploads/2019/03/CTC-SENTINEL-032019.pdf>.

⁹⁷⁹ Petter Nesser, “Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs” CTC Sentinel, May 2019. Accessed August 4, 2020. <https://ctc.usma.edu/wp-content/uploads/2019/03/CTC-SENTINEL-032019.pdf>.

⁹⁸⁰ Scott Gates and Sukanya Podder, “Social Media, Recruitment, Allegiance and the Islamic State” (Perspective on Terrorism, 2015) 107–113.

⁹⁸¹ Scott Gates and Sukanya Podder, “Social Media, Recruitment, Allegiance and the Islamic State” (Perspective on Terrorism, 2015) 107–113.

⁹⁸² Scott Gates and Sukanya Podder, “Social Media, Recruitment, Allegiance and the Islamic State” (Perspective on Terrorism, 2015) 107–113.

countries in the Maghreb.”^{983, 984}. Whether foreign fighters are from the EU, Middle East, Gulf, or South/Southeast Asia, they all pose a threat to the country they get to in terms of security, because of the extremist ideology and views of the world compared to their views of how the world should see them and fear them.

Financing

The Islamic State is one of the biggest and richest terrorist organizations in the world. The net worth comes to about \$2 billion dollars⁹⁸⁵. This stems from natural resources, taxation, smuggling artifacts/art, human trafficking and extortion methods. There is a hierarchical design to the way the Islamic State operates that includes “separating revenue collection activities from disbursement and management.”⁹⁸⁶. One of the key aspects to limiting the Islamic State from gaining power is to expel their financial connections.

Counter-terrorist organizations have developed methods to shed light on how terrorist organizations such as IS are able to maximize their financial stability. As an example, al-Qaeda depended on reverse money laundering or channeling funds through Islamic charities and legitimate business to fund its military council. Due to the recognition of increased counter-terrorism measures, more than 165 countries had multiple assets frozen of individuals and organizations that were potentially connected to terrorism groups⁹⁸⁷. Limiting their finances will result in a blow to their resources and economic funding. The Islamic State is set up in a way which is formed

⁹⁸³ Maghreb includes Northwest Africa and the western part of the Arab world which is predominantly Muslim. The countries included: Algeria, Libya, Egypt, Mali, Niger, Sudan, Nigeria, Chad, Morocco, and Tunisia.

⁹⁸⁴ Scott Gates and Sukanya Podder, “Social Media, Recruitment, Allegiance and the Islamic State” *Perspective on Terrorism*, (2015): 107–113.

⁹⁸⁵ Rafat Kurdi, “Islamic State”, (November 2016) https://www.amo.cz/wp-content/uploads/2016/11/NATO_isis_final.pdf website accessed + date.

⁹⁸⁶ Luigi Achilli and Alessandro Tinti, “Debunking the smuggler-terrorist nexus: human smuggling and the Islamic State in the Middle East”, *European University Institute*, October 28, 2019. Accessed July 28, 2020, <https://www.tandfonline.com/doi/abs/10.1080/1057610X.2019.1678884?journalCode=uter20>.

⁹⁸⁷ Peng Wang, “The Crime-Terror Nexus: Transformation, Alliance, Convergence”, *Asian Social Science*, (2010): 11–18.

much like a cabinet. IS has assembled a “financial committee consisting of a finance minister who oversees its financial affairs and exerts authority over local finance councils for the provinces... The primary purpose of the finance minister is to ensure tax collection is met.”⁹⁸⁸. Dissolving their financial system is a key strategy used to limit the power of the Islamic State. For instance, the US led coalition in Syria caused IS to lose a lot of its land power. This resulted in the depleted income of the terrorist organization. Formerly in 2017, the Islamic State controlled around “23,300 square miles of territory between Iraq and Syria.”⁹⁸⁹. However, a 2019 report stated “IS has lost control of almost all of its territory due to joint military campaigns”⁹⁹⁰, with control only over discrete amounts of “land in eastern Syria near the Iraqi border”⁹⁹¹. This estimates to about “9,300 square miles of land resulting in a 96%”⁹⁹² reduction of land and valuable means of financial stability. From the shrinkage of land power, the methods used to retain their financial stability is still at large.

Oil

IS controls many areas within Iraq and Syria with a wide range of industrial opportunities such as natural resources and raw materials indigenous to the land. One of these resources is oil. In 2014, around 350 oil wells in Iraq and 60% of Syria’s oil fields were overtaken by the Islamic State⁹⁹³. One

⁹⁸⁸ Center for the Analysis of Terrorism, “ISIS Financing”, May 2016. Accessed August 11, 2020. <https://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf>.

⁹⁸⁹ Aljazeera, “After the almost 100 percent defeat of ISIS, what about its ideology?” May 8, 2018. Accessed August 11, 2020, <https://studies.aljazeera.net/en/reports/2018/05/100-percent-defeat-isis-ideology-180508042421376.html>.

⁹⁹⁰ Ari Shapiro, “The Current State of ISIS as Its END Draws Near” February 19, 2019. Accessed September 19, 2020, <https://www.npr.org/2019/02/19/696075305/the-current-state-of-isis-as-its-end-draws-near>.

⁹⁹¹ Ari Shapiro, “The Current State of ISIS as Its END Draws Near” February 19, 2019. Accessed September 19, 2020, <https://www.npr.org/2019/02/19/696075305/the-current-state-of-isis-as-its-end-draws-near>.

⁹⁹² Aljazeera, “After the almost 100 percent defeat of ISIS, what about its ideology?” May 8, 2018. Accessed August 11, 2020, <https://studies.aljazeera.net/en/reports/2018/05/100-percent-defeat-isis-ideology-180508042421376.html>.

⁹⁹³ Matthew Levitt, “Terrorist Financing and the Islamic State” Washington Institute for Near East Policy, November 13, 2014. Accessed July 31, 2020. <https://www.washingtoninstitute.org/uploads/Documents/testimony/LevittTestimony20141113.pdf>.

report suggests, “The exploitation of the natural reserves of oil refineries constitutes of one of several primary sources of funding.”⁹⁹⁴ This has enabled IS to be one of the most powerful and richest terrorist organizations in the world⁹⁹⁵. The Islamic State makes an earning approximately worth “\$500 million a year”⁹⁹⁶ from the oil refineries alone. Through black-market sales and local truck drivers in the region, they are able to then smuggle, export and transport oil through backhanded deals to sell the oil and deliver it to its final destination to countries such as Jordan, Turkey, Iran, and Kurdistan⁹⁹⁷. The war in Syria in 2015, significantly reduced the amount earned from the oil refineries from key territories. In 2014, the earnings from oil equated to “\$1 billion compared to in 2015 which the income earned was estimated about \$600 million dollars.”⁹⁹⁸ However, due to the recent loss of territory, IS’s revenues have become strained as the value of oil barrels being sold has decreased, as well as the yearly income gained. By limiting the finances of the Islamic State, it will effectively hurt the operations of the organization.

Taxation

Tax earnings by the IS are worth approximately over \$250 million a year⁹⁹⁹. The taxes are imposed on the civilians living in the cities under IS control. IS imposes an additional tax on non-Muslims – *Jizyah*¹⁰⁰⁰. IS has been able to tax almost everything which includes, but is not limited to, agricultural

⁹⁹⁴ Center for the Analysis of Terrorism, “ISIS Financing”, May 2016. Accessed August 11, 2020. <https://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf>.

⁹⁹⁵ Rafat Kurdi, “Islamic State”, (2016) https://www.amo.cz/wp-content/uploads/2016/11/NATO_isis_final.pdf.

⁹⁹⁶ Rafat Kurdi, “Islamic State”, (2016) https://www.amo.cz/wp-content/uploads/2016/11/NATO_isis_final.pdf.

⁹⁹⁷ Jean-Charles Brisard and Damien Martinez, “Islamic State: the economy-based terrorist funding”, October 2014. Accessed August 4, 2020. <http://www.gdr-elsj.eu/wp-content/uploads/2015/11/Islamic-State.pdf>.

⁹⁹⁸ Center for the Analysis of Terrorism, “ISIS Financing”, May 2016. Accessed August 11, 2020. <https://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf>.

⁹⁹⁹ Center for the Analysis of Terrorism, “ISIS Financing”, May 2016. Accessed August 11, 2020. <https://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf>.

¹⁰⁰⁰ *Jizyah*: a yearly additional tax imposed on those who are non-Muslims who are not willing or wanting to convert.

goods, telecommunication companies, cash withdrawals from bank accounts, road tax, custom per truck entering Jordan and Syria border checks, looting archeological sites, and protection tax¹⁰⁰¹. In 2015 this resulted in a \$250 million earning¹⁰⁰². The money earned from all the taxes have been put towards expansion into new territories within the region IS has claimed in Syria and Iraq and an “extensive civil system”, especially to “fund garbage collectors and motor vehicle authority.”¹⁰⁰³. There are fees placed upon each household per month for the essential items (i.e. water and electricity). The fees for each household made about \$60 million in 2015¹⁰⁰⁴. In terms of human trafficking, IS also taxes the “greedy bogeymen”¹⁰⁰⁵ who facilitate in criminal cartels with smuggling route passage fees “to move goods across the area under the Caliphate’s de-facto jurisdiction”¹⁰⁰⁶. This was done so IS could gain income as well as new potential recruits.

Smuggling Arts/Artifacts

Iraq and Syria have important (incl. UNESCO Word Heritage) archeological sites that consist of cultural artifacts dating back 9,000 BCE. IS has taken these ancient historical artifacts and produced revenue from selling them. The Site of Palmyra for example, located in the Syrian desert, north-east of Damascus, represents an archeological heritage site of the ancient world,

¹⁰⁰¹ Jean-Charles Brisard and Damien Martinez, “Islamic State: the economy-based terrorist funding”, October 2014. Accessed August 4, 2020. <http://www.gdr-elsj.eu/wp-content/uploads/2015/11/Islamic-State.pdf>.

¹⁰⁰² Center for the Analysis of Terrorism, “ISIS Financing”, May 2016. Accessed August 11, 2020. <https://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf>.

¹⁰⁰³ Rosie Perper, “ISIS made millions from taxes that it then used to run garbage collections and even a DMV” Business Insider, April 6, 2018. Accessed August 9, 2020, <https://www.businessinsider.com/islamic-state-used-taxes-to-grow-power-and-offer-services-2018-4>.

¹⁰⁰⁴ Center for the Analysis of Terrorism, “ISIS Financing”, May 2016. Accessed August 11, 2020. <https://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf>.

¹⁰⁰⁵ Luigi Achilli and Alessandro Tinti, “Debunking the smuggler-terrorist nexus: human smuggling and the Islamic State in the Middle East”, European University Institute, October 28, 2019. Accessed July 28, 2020, <https://www.tandfonline.com/doi/abs/10.1080/1057610X.2019.1678884?journalCode=uter20>.

¹⁰⁰⁶ Luigi Achilli and Alessandro Tinti, “Debunking the smuggler-terrorist nexus: human smuggling and the Islamic State in the Middle East”, European University Institute, October 28, 2019. Accessed July 28, 2020. <https://www.tandfonline.com/doi/abs/10.1080/1057610X.2019.1678884?journalCode=uter20>.

with Graeco- Roman and Persian influences¹⁰⁰⁷. IS has made an estimated \$30 million to \$50 million dollars a year from selling artifacts from these cultural heritage sites¹⁰⁰⁸. Smuggling artifacts and/or art items, as well as “taxing looted antiquities”¹⁰⁰⁹ is one of the economic sources that finances the Islamic State by a large income worth. Any items found are subjected to taxes ranging from 20% to 50%¹⁰¹⁰. To make money from these artifacts, IS “smuggle[s] them into Europe via Turkey, Jordan, Iran, and Syria”¹⁰¹¹ sales and/or auctions them internationally. IS has created a systematic structure to obtain the financials of the looted and smuggled artifacts by creating an antique department within the ministry of natural resources, and legalizing the looting of the archeological sites of these artifacts¹⁰¹². Documents supporting this ministry highlights the cultural antiques preparation for professional sale internationally. Since 2014, the United Nations Security Council (UNSC) monitoring team enacted sanction and recommendations to Member States in order to hopefully disrupt the financing of IS and the sale of cultural artifacts¹⁰¹³. It remains unknown how much they are earn-

¹⁰⁰⁷ UNESCO, “Site of Palmyra”, 2020. Accessed September 19, 2020, <https://whc.unesco.org/en/list/23/>.

¹⁰⁰⁸ Rafat Kurdi, “Islamic State” Listopad, (2016) https://www.amo.cz/wp-content/uploads/2016/11/NATO_isis_final.pdf.

¹⁰⁰⁹ Hans-Jakob Schindler & Frederique Gautier, “Looting and smuggling of artifacts as a strategy to finance terrorism global sanction as a disruptive and preventive tool”, *International Journal of Cultural Property*, September 2, 2019. Date Accessed July 31, 2020, <https://www.cambridge.org/core/journals/international-journal-of-cultural-property/article/looting-and-smuggling-of-artifacts-as-a-strategy-to-finance-terrorism-global-sanctions-as-a-disruptive-and-preventive-tool/3485D8F8BF5EC709D85ECACBDA4E6972>.

¹⁰¹⁰ Center for the Analysis of Terrorism, “ISIS Financing”, May 2016. Accessed August 11, 2020. <https://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf>.

¹⁰¹¹ Matthew Levitt, “Terrorist Financing and the Islamic State” Washington Institute for Near East Policy, November 13, 2014. Accessed July 31, 2020. <https://www.washingtoninstitute.org/uploads/Documents/testimony/LevittTestimony20141113.pdf>.

¹⁰¹² Hans-Jakob Schindler & Frederique Gautier, “Looting and smuggling of artifacts as a strategy to finance terrorism global sanction as a disruptive and preventive tool”, *International Journal of Cultural Property*, September 2, 2019. Accessed July 31, 2020, <https://www.cambridge.org/core/journals/international-journal-of-cultural-property/article/looting-and-smuggling-of-artifacts-as-a-strategy-to-finance-terrorism-global-sanctions-as-a-disruptive-and-preventive-tool/3485D8F8BF5EC709D85ECACBDA4E6972>.

¹⁰¹³ Hans-Jakob Schindler & Frederique Gautier, “Looting and smuggling of artifacts as a strategy to financeterroismglobalsanctionasadisruptiveandpreventivetool”, *International Journal of Cultural Property*, September 2, 2019. Accessed July 31, 2020, <https://www.cambridge.org/core/journals/international-journal-of-cultural-property/article/looting-and-smuggling-of-artifacts-as-a-strategy-to-finance-terrorism-global-sanctions-as-a-disruptive-and-preventive-tool/3485D8F8BF5EC709D85ECACBDA4E6972>.

ing in recent years from the sale of historical artifacts/antiques sold on the black-market to make from outside sources.

Human Trafficking

The American Intelligence Journal reports, “human trafficking is one of the fastest growing illicit activities in the world, and is second most profitable crime along with weapons and drugs”¹⁰¹⁴. Human trafficking is one aspect of illicit activities that usually accompanies other criminal activities (i.e. drug trafficking). The act of human trafficking is usually smuggling persons who were into the process. Some of the prominent elements of human trafficking include: 1) the act (i.e harboring, recruiting, and transporting), 2) the means (i.e. “forced, deceived, coerced or exploited”)¹⁰¹⁵, and 3) the purpose (i.e. exploitation and gain).

With the uprise in the irregular migration flow, human trafficking became a lucrative business for smugglers, terrorist organizations, and illegal organizations. The logistics of human trafficking requires investment for networking, warehousing of the victims, inspection, modes of transportation, and partnerships with other organizations for the purchase of the victims.

The Islamic State takes part in the trafficking of humans, especially women and children. Acts of sexual and gender-based violence has been a strategic objective of terrorist groups¹⁰¹⁶. For example, Yazidi were targeted by IS, whereby Yazidi women and young girls were sold for sexual abuse and/or family housekeepers, and male children used as new recruits for combat and support roles (e.g. human shields, informants, bombmakers, executioners, and suicide bombers) by IS inserting its ideology from a young age. In 2017, IS abducted 400 Yazidi children for combat training roles. IS has enacted

¹⁰¹⁴ Daniels Sheinis, “The Links Between Human Trafficking, Organized Crime, and Terrorism”. American Intelligence Journal 30, no. 1 (2012): 68–77. Accessed August 11, 2020, www.jstor.org/stable/26201986.

¹⁰¹⁵ Daniels Sheinis, “The Links Between Human Trafficking, Organized Crime, and Terrorism”. American Intelligence Journal 30, no. 1 (2012): 68–77. Accessed August 11, 2020, www.jstor.org/stable/26201986.

¹⁰¹⁶ United Nations Security Council, “Identifying and Exploring the Nexus between Human Trafficking, Terrorism, and Terrorism Financing”, November 15, 2018. Accessed September 23, 2020. <https://www.un.org/sc/ctc/wp-content/uploads/2019/02/HT-terrorism-nexus-CTED-report.pdf>.

heinous crimes towards the persons of other religious cultures committing mass crime, “ethnic cleansing campaigns”¹⁰¹⁷, and enslaving them. Human trafficking may not be as profitable as other parts of the Islamic State finances, but the selling of humans as “commodities”¹⁰¹⁸ has proven to be beneficial by exploiting financial gain of ransom money towards families. The demanded prices of ransom has ranged between \$10,000-\$40,000. In 2014 IS made between \$35 to \$45 million¹⁰¹⁹. As Achilli and Tinti stated, this has become a “dirty entanglement”¹⁰²⁰ for a more lucrative economic and social opportunity to expand their resources.

The methods IS uses, combined with efforts of migrant smugglers, has generated income from the business through taxes, selling of women and children, and slave labor. IS has benefited from the partnership from an economic standpoint, as well as learning the routes which the smugglers use to try to gain access to Europe. If they were to get involved in the business, “EUROPOL estimated that the flow of irregular migration would have amounted to an income between EUR 3 to 6 billion.”¹⁰²¹.

Border Security in the European Union in the Context of Terrorist Threats

Migration

Within the EU, migration has accelerated between 2015–2017. The numbers of asylum seekers, refugees and migrants rose quickly. Between 2014–2017 more than 919,000 Syrians applied for asylum within the EU

¹⁰¹⁷ Ibid.

¹⁰¹⁸ Ibid.

¹⁰¹⁹ Ibid.

¹⁰²⁰ Luigi Achilli and Alessandro Tinti, “Debunking the smuggler-terrorist nexus: human smuggling and the Islamic State in the Middle East”, European University Institute, October 28, 2019. Accessed July 28, 2020. <https://www.tandfonline.com/doi/abs/10.1080/1057610X.2019.1678884?journalCode=uter20>.

¹⁰²¹ Luigi Achilli and Alessandro Tinti, “Debunking the smuggler-terrorist nexus: human smuggling and the Islamic State in the Middle East”, European University Institute, October 28, 2019. Accessed July 28, 2020. <https://www.tandfonline.com/doi/abs/10.1080/1057610X.2019.1678884?journalCode=uter20>.

alone¹⁰²². With the increase in geopolitical turmoil overseas in the Middle East and North African regions, the demand has increased for immigrants wanting to come to the EU. The number of refugees surpassed the number of migrants travelling to the EU within the past 5 years. Since 2015, the migration and refugee crisis has amounted to 2.4 million refugees and 860 thousand asylum seekers as cases are pending at the end of 2018¹⁰²³. Demands to accommodate and manage the essential information needed from the migrants and refugees resulted in the development of a database system created to inform policy makers and the public. With the help of these databases, countries are now able to analyze, assess threat levels, provide socio-economic indicators, and provide regulations for the migration public and asylum seekers.

In regard to security measures, migration will always be deemed as a risk. Many people wanting to enter the EU may be flagged for connections with terrorist organizations, affiliated in criminal activity, smuggling illegal or illicit goods, or may be wanted by other countries¹⁰²⁴. During the conflict in Syria in 2015, IS took this “opportunity to try and smuggle in operatives among the migrants or refugees to mobilize connections overseas and recruit members.”¹⁰²⁵. This also provided the opportunity for foreign fighters to travel abroad to fight in conflicts for certain terrorist organizations. This has created concerns regarding foreign fighters returning home. Due to the increased risk of terrorist attacks, the EU has put in place strategies, security agencies such as ECTC, FRONTEX, and enhanced capabilities to use more advanced technological equipment for identification, centers for terrorism and radicalization awareness to warn and inform the public.

¹⁰²² BBC News, “Migration to Europe in Charts”, September 18, 2018. Accessed September 26, 2020. <https://www.bbc.com/news/world-europe-44660699>.

¹⁰²³ Migration Data Portal, “Migration data in Europe,” August 3, 2020. Accessed August 11, 2020. <https://migrationdataportal.org/regional-data-overview/europe>.

¹⁰²⁴ FRONTEX, “Risk Analysis 2020”, March 2020. Accessed July 20, 2020. https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Annual_Risk_Analysis_2020.pdf.

¹⁰²⁵ Petter Nesser, “Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs” CTC Sentinel, May 2019. Accessed August 4, 2020. <https://ctc.usma.edu/wp-content/uploads/2019/03/CTC-SENTINEL-032019.pdf>.

EU Counter Terrorism Strategy

Security measures rose after the 9/11 terrorist attacks in the US, which enhanced the protocols that are in place today in Europe and the US. However, a turning point for more assertive collaboration within the EU to prevent terrorist attacks came following the terrorist attack bombing in Madrid in 2004. Effective immediately, the EU Counter-Terrorism Strategy was created to boost the security measures of the EU. The basis of the strategy are based upon “four pillars of prevent, protect, pursue, and respond”¹⁰²⁶. and “5 main objectives regarding the counter-terrorism border strategies: strengthening external border controls, enhancing capacities for identifying terrorist at border, improving identity document security, strengthening the exchange of information relating to border controls, and coordinating the reintroduction of internal border controls.”¹⁰²⁷. In recent times the threat may no longer be physical, but more of a mix of physical and electronic (i.e. hybrid). Potential terrorist threats are becoming complex, this allows for organized crime or terrorist organizations such as the Islamic State to make connections based upon both platforms to exploit anyone for their own gain. These threats may “happen outside of the EU borders, but can still affect what may have critical impact on the security inside the EU.”¹⁰²⁸. Europol reports, “Recently IS has transitioned to a covert insurgent group operating in Iraq and Syria and maintained its global network connections.”¹⁰²⁹. An example of this mixture would be the entrepreneurs of the Islamic State which use electronic methods to communicate with other radicals, foreign fighters, or new recruits to supply them information or any type of plans to make a threat a reality within a country. Coopera-

¹⁰²⁶ Sarah Léonard, “Border Controls as a dimension of the European Union’s counter-terrorism policy: a critical assessment,” January 13, 2015, *Intelligence and National Security* 30, no. 2–3 (2015): 306–332.

¹⁰²⁷ Ibid.

¹⁰²⁸ European Commission, “Communication from the commission to the European parliament, the European council, the council, the European economic and social committee and the committee of the regions” July 24, 2020. Accessed August 11, 2020. <https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf>.

¹⁰²⁹ Europol, “Terrorism”, 2020. Accessed August 12, 2020. <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/terrorism>.

tion between all Member States¹⁰³⁰ is a key aspect to the security of the EU to fight the increase in terrorism within the regions. The fight against terrorism will start with the “cooperation with third countries and at global level to address common challenges in the EU.”¹⁰³¹

European Border and Coast Guard Agency (FRONTEX)

FRONTEX and the European Counter Terrorism Centre at Europol work towards “safeguarding the area of freedom, justice, and security.”¹⁰³² The purpose of FRONTEX is to safeguard the borders of the EU. Frontex states, “Member States reported an increase in the detection of clandestine or secondary movement entries on both inland and sea routes in 2019, but a decrease in illegal border crossing along the external borders in 2019 compared to 2013.”¹⁰³³ In 2019, FRONTEX reported the top 3 nationalities for migration and refugees: Afghanistan with 34,154, Syria with 24,390, and Morocco with 8,020¹⁰³⁴. There are several routes used by different nationalities depending on the region they are coming from. For instance, the Western Balkan Route consist of migrants or refugees coming from Afghanistan, Syria, and Iraq, whereas the Central Mediterranean route accompany migrants and refugees from Tunisia, Sudan, and Côte d’Ivoire. The migration flow is monitored and recorded by FRONTEX, to safeguard border security, entry, documentation, and cross border crime from different migration routes. The reason why there is sizable amount of security when it comes to the border of the EU is due to the fact that sometimes in the mix of migrants or refugees there are persons who are red listed for criminal and dangerous activities they have been involved in. FRONTEX

¹⁰³⁰ Member States: countries that originally started out to working economically in 1951 were Belgium, Germany, France, Luxembourg, Italy, and the Netherlands. Now there are 27 countries that are part of the Member States in the EU, excluding the UK who withdrew in January 2020.

¹⁰³¹ European Commission, “Communication from the commission to the European parliament, the European council, the council, the European economic and social committee and the committee of the regions” July 24, 2020. Accessed August 11, 2020. <https://ec.europa.eu/info/sites/info/files/communication-eu-security-union-strategy.pdf>.

¹⁰³² FRONTEX, “Risk Analysis 2020”, March 2020. Accessed July 20, 2020. https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Annual_Risk_Analysis_2020.pdf.

¹⁰³³ Ibid.

¹⁰³⁴ Ibid.

is there to protect the citizens of the EU from any potential threats from entering. They do this by checking for illegal items which most often come in the form of illegal firearms, drug trafficking, stolen vehicles and parts, and false documentation. FRONTEX admits, “Borders provide challenges, but also opportunities in countering-terrorism as they offer a geographical spread where Member States can take executive actions to deter, disrupt, and detect terrorist-related movements and detain those involved in terrorist-related activities.”¹⁰³⁵.

Advanced technological programs such as the Schengen Information System (SIS), Entry-Exit System (EES), and the Electronic Travel Information and Authorization (ETIAS) are technical identification informational systems that help with the fight against terrorism or terror-related activities/persons¹⁰³⁶. The support system of FRONTEX has four guidelines towards their mission: a) adapting to the threat and facilitating access, b) outreaching and spreading knowledge, c) engaging and supporting, and d) informing/influencing EU policy¹⁰³⁷. All these efforts to support in countering-terrorism are to make the process for the entire EU work as a team for the same goal of protection and safety of each nation.

European Counter Terrorism Centre (ECTC) at Europol

One of the priorities for ECTC is to counter the advancement of terrorism as well as foreign fighters. Despite threatening plots and attacks in the EU in recent years, the EU Situation and Trend Report (TESAT) states, “a total of 199 completed, failed, and foiled terrorist attacks in 2019 were reported by 13 EU countries”¹⁰³⁸. The capability of the Islamic State to create contact networks of extremist within the EU and the Middle East causes ad-

¹⁰³⁵ Ibid.

¹⁰³⁶ Sarah Léonard, “Border Controls as a dimension of the European Union’s counter-terrorism policy: a critical assessment,” January 13, 2015, *Intelligence and National Security* 30, no. 2–3 (2015): 306–332.

¹⁰³⁷ FRONTEX, “Risk Analysis 2020”, March 2020. Accessed July 20, 2020. https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Annual_Risk_Analysis_2020.pdf.

¹⁰³⁸ Europol, “European Terrorism Situation and Trend Report (TESAT)”, 2020. Accessed August 13, 2020. <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/terrorism>.

ditional threats of terrorism. Europol shares, “The European Counter Terrorism Centre (ECTC) evolved in 2016 to enhance cross border cooperation between relevant counter-terrorism authorities.”¹⁰³⁹ The Report goes on to argue, “Terrorist attacks tend to be directed by IS or inspired by IS ideology and rhetoric that include a range of weapons that include bladed weapons, automatic rifles, explosives, and vehicles.”¹⁰⁴⁰ While the threat of terrorism has subsided in 2019 because of the effective law enforcement and security authorities, there is still a high demand for safe security measures. While FRONTEX focuses on the border security aspect, ECTC works on countering terrorism within the EU countries. This includes migrants who may have been turned by persuasion of an IS affiliate, the radicalism in prisons that can lead to recruitment, and sole actors who are persuaded by e.g. martyr and heroic ideologies. These threats remain high within the EU¹⁰⁴¹. Terrorism Situation and Trends report states that in 2019 there were 1,004 individuals arrested on suspicion of terror-related activities in 19 Member States¹⁰⁴². That number has decreased from 2017, which reported 1,219¹⁰⁴³ arrests on suspicion of terrorist-related activities. Security measures are placed by ECTC to keep the public safe from any potential harm and Europol works towards that goal to subside violent tactics by extremist whether they are sole actors or from an organization.

The Radicalization Awareness Network (RAN)

As part of the EU Internal Security Strategy (EU ISS) in 2010, its main objective is to target radicalization and recruitment. By 2017 the pressure to reform the prison system to combat criminalization of terrorism increased with the newly adopted EU Directive on combatting terrorism¹⁰⁴⁴. Radicali-

¹⁰³⁹ Ibid.

¹⁰⁴⁰ Ibid.

¹⁰⁴¹ Scott Gates and Sukanya Podder, “Social Media, Recruitment, Allegiance and the Islamic State” *Perspective on Terrorism*, (2015): 107–113.

¹⁰⁴² Europol, “European Terrorism Situation and Trend Report (TESAT)”, 2020. Accessed August 13, 2020. <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/terrorism>.

¹⁰⁴³ Ibid.

¹⁰⁴⁴ ICF, “How to prevent dangerous radicalization in prisons”, March 4, 2019. Accessed September 22, 2020. <https://www.icf.com/insights/public-policy/preventing-radicalization-in-prisons>.

zation of criminals occurring in prisons has become a focus point for the RAN organization¹⁰⁴⁵. This is where terrorist-related activities, return of foreign fighters, and criminals tend to congregate and end up sharing some of the same ideologies and/or looking for new life once out of prison, all of which the Islamic State tapped into as part of its newer recruiting methods. An ICF report suggests, “The prison environment helped European terrorist groups support and further develop propaganda, as well as extremist groups from the conditions of the prisons”¹⁰⁴⁶.

In response to these findings, Radicalization Awareness Network (RAN) was created, as a network of practitioners and experts working towards preventing and countering violent extremism. With the support of the European Organization of Prison and Correctional Services (EUOPRIS), they work towards the de-radicalization and prevention of radicalization in prisons¹⁰⁴⁷. In 2015, the key focal point of RAN was to “develop work with third countries with a priority on Turkey, and countries in the Middle East, Western Balkans, and North Africa.”¹⁰⁴⁸. Working towards de-radicalization in prisons is a top priority as a fight against terrorism from within the Member States.

Conclusion

Terrorist organizations and terrorist threats are security issues for all countries. When the terrorist attacks happened in the US on September 11,

¹⁰⁴⁵ European Commission, “Communication from the commission to the European parliament, the European council, the council, the European economic and social committee and the committee of the regions”, April 24, 2015. Accessed July 31, 2020. <https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf>.

¹⁰⁴⁶ ICF, “How to prevent dangerous radicalization in prisons”, March 4, 2019. Accessed September 22, 2020. <https://www.icf.com/insights/public-policy/preventing-radicalization-in-prisons>.

¹⁰⁴⁷ European Commission, “Communication from the commission to the European parliament, the European council, the council, the European economic and social committee and the committee of the regions”, April 24, 2015. Accessed July 31, 2020. <https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf>.

¹⁰⁴⁸ European Commission, “Communication from the commission to the European parliament, the European council, the council, the European economic and social committee and the committee of the regions”, April 24, 2015. Accessed July 31, 2020. <https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf>.

2001, it set a standard for increased security measures. When the attack happened in the EU in Madrid in 2004, that set the tone for the EU to take counter measures towards the fight against terrorism. The terror, fear, and uncertainty of the Islamic State's future plans has pushed the EU to increase security measures to prevent terrorist attacks. By 2006, the EU formed FRONTEX to protect its borders and control the internal and external border management of migration from land and sea, refugees, and the stoppage of illegal firearms, drug trafficking, and illicit goods. With the migration and refugee crisis that took place in 2015, IS took advantage of this opportunity to smuggle in operatives as well an increase in foreign fighters. This also stems from the motivation and propaganda used to bring more persons for foreign land to be recruited into the Islamic State. Over the past couple of years many foreign fighters returning from their combat tour have "avowedly reject[ed] the Islamic State and its violent ways/tactics."¹⁰⁴⁹ The downward trend in 2019 from terrorist attacks and plots foiled, a decrease in foreign fighters traveling to and from countries with known conflicts, as well as a decrease in terror-related activities, and radicalism has shown that the fight against terrorism is effective. The depletion of the Islamic State finances from land lost due to the formation of joint coalitions to deter IS over in Syria and Iraq have effectively minimized their resources. Although their main sources of oil and taxes are less, they are still able to network through telecommunications with recruiters and other foreign fighters all over the world. With the downward trend of plots and/or attacks by terrorist, the goal within the security challenges for the EU for the next five years should focus on three main areas:

1. fighting organized crime,
2. countering terrorism and radicalization,
3. fighting crimes in the digital age"¹⁰⁵⁰.

¹⁰⁴⁹ Souad Mekhennet and Joby Warrick, "The appeal of ISIS fades among Europeans who return home from Syria", Washington Post, June 14, 2020. Accessed August 10, 2020. https://www.washingtonpost.com/national-security/the-appeal-of-isis-fades-among-europeans-who-returned-home-from-syria/2020/06/14/754b3e0e-acb9-11ea-9063-e69bd6520940_story.html.

¹⁰⁵⁰ European Commission, "Security Union Strategy", Migration and Home Affairs, July 2020. Accessed August 12, 2020. https://ec.europa.eu/home-affairs/what-we-do/policies/security-union-strategy_en.

Although it is hard to determine for how long this downward trend of terrorist attacks will continue, the continuous progression towards the security of the EU, the fight against radicalism, and the help provided to third countries from the influence of terrorist organizations can keep the amount of threats and progression minimized.

Bibliography

- “After The “Almost 100 Percent” Defeat Of ISIS, What About Its Ideology? | Al Jazeera Center for Studies”. 2018. *Al Jazeera Center for Studies*. <https://studies.aljazeera.net/en/reports/2018/05/100-percent-defeat-isis-ideology-180508042421376.html>.
- “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and The Committee of the Regions the European Agenda on Security”. 2015. *Cepol.Europa.Eu*. <https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf>.
- “ISIS Financing”. 2016. *Cat-Int.Org*. <https://cat-int.org/wp-content/uploads/2016/06/ISIS-Financing-2015-Report.pdf>.
- “Migration Data In Europe”. 2020. *Migration Data Portal*. <https://migrationdata-portal.org/regional-data-overview/europe>.
- “Risk Analysis For 2020”. 2020. *Frontex.Europa.Eu*. https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Annual_Risk_Analysis_2020.pdf.
- “Syrian Refugee Crisis: Facts, Faqs, And How To Help | World Vision”. 2020. *World Vision*. <https://www.worldvision.org/refugees-news-stories/syrian-refugee-crisis-facts>.
- “Terrorism”. 2020. *Europol*. <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/terrorism>.
- “TESAT”. 2020. *Terrorism TESAT*. <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/terrorism>.
- “The War Against ‘Islamic State’ In Maps And Charts”. 2020. *BBC News*. <https://www.bbc.com/news/world-middle-east-27838034>.

- "Who Are The European Jihadis? From Criminals To Terrorists And Back? Midterm Report – GLOBSEC". 2018. *GLOBSEC*. <https://www.globsec.org/publications/who-are-european-jihadis-from-criminals-to-terrorists-and-back/>.
- "Identifying and Exploring the Nexus between Human Trafficking, Terrorism, and Terrorism Financing." Counter-Terrorism Committee Executive Directorate, United Nations Security Council, 15 Nov. 2018, www.un.org/sc/ctc/wp-content/uploads/2019/02/HT-terrorism-nexus-CTED-report.pdf.
- "2019 World Press Freedom Index – A Cycle of Fear", April 21, 2020. <https://rsf.org/en/2019-world-press-freedom-index-cycle-fear>.
- "2020 Edelman Trust Barometer." Edelman, 2020. <https://www.edelman.com/trustbarometer>.
- "A Rift in Democratic Attitudes Is Opening up around the World." *The Economist*, August 22, 2020. <https://www.economist.com/graphic-detail/2020/08/22/a-rift-in-democratic-attitudes-is-opening-up-around-the-world>.
- "About the PSIA", PSIA | 公安調査庁 (Public Security Intelligence Agency, 2020), <http://www.moj.go.jp/psia/English.html>.
- "Actors and Tactics of Conflict Interventions (Civilian Intervention and Nonviolent Intervention)." Irénées: A Website of Resources for Peace. Accessed August 25, 2020. http://www.irenees.net/bdf_fiche-analyse-659_en.html.
- "Career Track Recruitment", Public Security Intelligence Agency (Public Security Intelligence Agency, 2020), <http://www.moj.go.jp/psia/sougou.html>.
- "Careers & Internships: Browse Jobs by Category", Central Intelligence Agency (Central Intelligence Agency, December 12, 2019), <https://www.cia.gov/careers/opportunities/cia-jobs/index.html>.
- "DOD Dictionary of Military and Associated Terms", www.jcs.mil (Joint Chiefs of Staff, June 2020), <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>, 181.
- "EL PAÍS: El Periódico Global." *EL PAÍS*, March 12, 2004. https://elpais.com/diario/2004/03/12/espana/1079046001_850215.html.
- "Firearms Directive". European Commission, accessed August 12th, 2020. https://ec.europa.eu/growth/sectors/firearms_en.
- "Foreign Terrorist Fighters – United Nations Security Council Counter-Terrorism Committee." United Nations. United Nations, 2014. <https://www.un.org/sc/ctc/focus-areas/foreign-terrorist-fighters/>.
- "Frank G. Hoffman." Foreign Policy Research Institute, May 7, 2020. <https://www.fpri.org/contributor/frank-hoffman/>.
- "How to Prevent Dangerous Radicalization in Prisons." ICF, ICF, 4 Mar. 2019, www.icf.com/insights/public-policy/preventing-radicalization-in-prisons.

- "Huawei and 5G – The European Theatre" *The Economist*, July 18, 2020.
- "In Memoriam: Ambassador John W. McDonald." United States Institute of Peace, May 30, 2019. <https://www.usip.org/press/2019/05/memoriam-ambassador-john-w-mcdonald>.
- "Information Warfare: Cyber Warfare Is the Future Warfare." *Global Information Assurance Certification Paper*, 2004.
- "Intelligence Analysis", RAND Corporation, accessed August 18, 2020, <https://www.rand.org/topics/intelligence-analysis.html>.
- "Iraqi Defense Market Outlook to 2024 – Iraqi Defense Expenditure Expected to Record a CAGR of 5.5% Over 2020–2024." GlobeNewswire News Room. Research and Markets, December 16, 2019. <https://www.globenewswire.com/news-release/2019/12/16/1961172/0/en/Iraqi-Defense-Market-Outlook-to-2024-Iraqi-Defense-Expenditure-Expected-to-Record-a-CAGR-of-5-5-Over-2020-2024.html>.
- "Is China Both a Source and Hub for International Students?" ChinaPower Project, March 12, 2020. <https://chinapower.csis.org/china-international-students/>.
- "Marine Corps Gazette." Marine Corps Gazette | Small Wars Journal. Accessed August 24, 2020. <https://smallwarsjournal.com/author/marine-corps-gazette>.
- "Mehdi Nemmouche", n.d. <https://www.counterextremism.com/extremists/mehdi-nemmouche>.
- "Member States Concerned by the Growing and Increasingly Transnational Threat of Right Wing Terrorism", United Nations, Accessed August 13th, 2020. https://www.un.org/sc/ctc/wp-content/uploads/2020/04/CTED_Trends_Alert_Extreme_Right-Wing_Terrorism.pdf.
- "Migration to Europe in Charts." BBC News, BBC, 11 Sept. 2018, www.bbc.com/news/world-europe-44660699.
- "NATO / OTAN." What is NATO? North Atlantic Treaty Organization. Accessed August 25, 2020. <https://www.nato.int/nato-welcome/index.html>.
- "Non-State Actors: Impact on International Relations and Implications for the United States." National Intelligence Council. National Intelligence Officer for Economics and Global Issues, August 23, 2007. https://www.dni.gov/files/documents/nonstate_actors_2007.pdf.
- "RAND Federally Funded Research and Development Centers (FFRDCs)", RAND Corporation, accessed August 18, 2020, <https://www.rand.org/about/ffrdc.html>.
- "Right-wing extremism" Bundesamt für Verfassungsschutz, accessed August 12th, 2020. <https://www.verfassungsschutz.de/en/fields-of-work/right-wing>

- extremism/figures-and-facts-right-wing-extremism/right-wing-extremist-demonstrations-2015.
- "State Actors – Actors in International Relations". Coursera. International Relations Theory. Accessed August 16, 2020. <https://www.coursera.org/lecture/international-relations-theory/state-actors-0GRQe>.
- "Stephen Blank". Foreign Policy Research Institute, April 24, 2020. <https://www.fpri.org/contributor/stephen-blank/>.
- "Steve Metz". Strategic Studies Institute. US Army War College. Accessed August 24, 2020. <https://ssi.armywarcollege.edu/faculty-staff/author-bio-metz/?q=543>.
- "Terrorism in the EU: Terror Attacks, Deaths and Arrests in 2019: News: European Parliament". Terrorism in the EU: terror attacks, deaths and arrests in 2019 | News | European Parliament. NEWS – European Parliament, July 14, 2020. <https://www.europarl.europa.eu/news/en/headlines/security/20180703STO07125/terrorism-in-the-eu-terror-attacks-deaths-and-arrests-in-2019>.
- "Terrorism Situation and Trend Report". TE SAT EUROPOL, 2017.
- "The 9/11 Commission Report", The 9/11 Commission Report § (2002), <https://govinfo.library.unt.edu/911/report/911Report.pdf>, 339–383.
- "The New Wave of Globalization and Its Economic Effects." World Bank, 2001.
- "War." Merriam-Webster. Merriam-Webster. Accessed August 24, 2020. <https://www.merriam-webster.com/dictionary/war>.
- "What Was OSS?" Central Intelligence Agency. Central Intelligence Agency, June 28, 2008. <https://www.cia.gov/library/publications/intelligence-history/oss/art03.htm>.
- "World Report 2020: Rights Trends in China's Global Threat to Human Rights", April 10, 2020. <https://www.hrw.org/world-report/2020/country-chapters/global>.
- A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* (Washington, DC: U.S. Government, 2009), <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf>.
- Abel, David. "Hackers kept allies on the defensive." *The Boston Globe*. June 20, 1999. Accessed August 11, 2020. <https://www.newspapers.com/image/441818908>.
- Abubakar, Aminu. "As Many as 200 Girls Abducted by Boko Haram, Nigerian Officials Say." *CNN*, April 16, 2014. <https://www.cnn.com/2014/04/15/world/africa/nigeria-girls-abducted/index.html>.
- Accessed August 14, 2020. <https://www.theatlantic.com/international/archive/2017/05/trump-declines-to-affirm-natos-article-5/528129/>.

- Achilli, Luigi, and Alessandro Tinti. "Debunking the Smuggler-Terrorist Nexus: Human Smuggling and the Islamic State in the Middle East." *Studies in Conflict & Terrorism* (2019): 1–16.
- Agamben, Giorgio. *State of Exception*. Chicago University Press, 2005.
- Ali, Javed. "Chemical Weapons and the Iran-Iraq War: A Case Study in Noncompliance" *The Nonproliferation Review/Spring*, 2001, Accessed August 11, 2020. <https://www.nonproliferation.org/wp-content/uploads/npr/81ali.pdf>.
- Allcott, Hunt, and Matthew Gentzkow. "Social Media and Fake News in the 2016 Election".
- Alter, Charlotte. "Girls Who Escaped Boko Haram Tell of Horrors in Captivity." *Time*, October 27, 2014. <https://time.com/3540263/girls-boko-haram-escape/>.
- Amos, Deborah. "Syrian War Crimes Trial Resumes In Germany." *NPR*, May 21, 2020. <https://www.npr.org/2020/05/21/859991380/syrian-war-crimes-trial-resumes-in-germany>.
- Anderson, Nick and Susan Svrluga. "Trump administration backs off plan requiring international students to take face-to-face classes." *The Washington Post*, July 14, 2020. Accessed August 17, 2020. https://www.washingtonpost.com/local/education/ice-rule-harvard-international-students-rescinded/2020/07/14/319fdae0-c607-11ea-a99f-3bbdfb1af38_story.html.
- Andréani, Gilles. "The 'War on terror': Good Cause, Wrong Concept". *Survival* 46, no. 4 (2004): 31–50.
- Andreeva, Christine. "EU Counter-terrorism Policy after 2015". *Institute of International & European Affairs (IIEA)*, (2019): 197–215. Accessed August 24, 2020, <https://www.iiea.com/wp-content/uploads/2019/06/Christine-Andreeva.pdf>
- Aning, Kwesi. "Confronting Hybrid Threats in Africa: Improving Multidimensional Responses." Essay. In *Future of African Peace Operations*, edited by Mustapha Abdallah, 20–37. The Nordic Africa Institute, 2016.
- Anzelmo, Erin L. "Cyberspace in International Law: Does the Internet Negate the Relevance of Territoriality in International Law?" *Studia Diplomatica* 58, no. 4 (2005), 155, <https://www.jstor.org/stable/44839534?seq=1>.
- Archer, John. "Does sexual selection explain human sex differences in aggression?" *Behavioral and Brain Sciences* 32, (2009): 249–311.
- Archer, John. "Sex Differences in Aggression in Real-World Settings: A Meta-Analytic Review." *Review of General Psychology* 8, (2004): 291–322.
- Argomaniz, Javier, Oldrich Bureš and Christian Kaunert. "A Decade of EU Counter-Terrorism and Intelligence: A Critical Assessment". *Intelligence and National Security* 30, no. 2–3 (2015): 191–206.

- Argomaniz, Javier. "When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms". *Journal of European Integration* 31, no. 1 (January 2009): 119–136.
- Aronofsky, David. "The War on Terror : Where We Have Been, Are, and Should Be Going". *Denver Journal of International Law & Policy* 40, no. 1 (April 2020): 90–105.
- Asperholm Hedlund, Laura. "Identifying and Understanding Anti-Immigration Disinformation: A case study of the 2018 Swedish national elections" (PhD diss., Swedish Defence University, 2019), 2019, 10, accessed August 4, 2020, <http://www.diva-portal.org/smash/get/diva2:1324745/FULLTEXT01.pdf>.
- Baddeley, Michelle C., Andrew Curtis, and Rachel Wood. "An Introduction to Prior Information Derived from Probabilistic Judgements: Elicitation of Knowledge, Cognitive Bias and Herding." *Geological Society, London, Special Publications* 239, no. 1 (2004): 15–27. <https://doi.org/10.1144/gsl.sp.2004.239.01.02>.
- Badey, Thomas J. "US counter-terrorism: Change in approach, continuity in policy". *Contemporary Security Policy* 27, no. 2 (2006): 308–324.
- Baldwin, Richard. *The Great Convergence: Information Technology and the New Globalization*. Cambridge, MA: Belknap Press of Harvard University Press, 2016.
- Balmas, Meital. "When Fake News Becomes Real: Combined Exposure to Multiple News Sources and Political Attitudes of Inefficacy, Alienation, and Cynicism." *Communication Research* 41, no. 3 (April 2014): 430–454. Accessed August 10, 2020. <https://doi.org/10.1177/0093650212453600>.
- Barkow, Jerome H., Leda Cosmides, and John Tooby, eds. *The adapted mind: Evolutionary psychology and the generation of culture*. Oxford University Press, USA, 1992. 163–229.
- Barrett, Brian. "Security News This Week: An Unprecedented Cyberattack Hit US Power Utilities." *Wired*. September 7, 2019. Accessed August 14, 2020. <https://www.wired.com/story/power-grid-cyberattack-facebook-phone-numbers-security-news/>.
- BBC News. "Europe and right-wing nationalism: A country-by-country guide." *BBC*, November 13, 2019. Accessed August 17, 2020. <https://www.bbc.com/news/world-europe-36130006>.
- BBC Technology. "How Russian bots appear in your timeline." *BBC*, November 14, 2017. Accessed August 8, 2020. <https://www.bbc.com/news/technology-41982569>.
- Beaujon, Andrew. "Trump Claims He Invented the Term 'Fake News' – Here's an Interview With the Guy Who Actually Helped Popularize It." *The Washingtonian*,

- October 2, 2019. Accessed August 9, 2020. <https://www.washingtonian.com/2019/10/02/trump-claims-he-invented-the-term-fake-news-an-interview-with-the-guy-who-actually-helped-popularize-it/>.
- Beaulieu, Brittany, and David Salvo. "NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence." *Alliance for Securing Democracy*, no. 031 (June 2018): 1–7.
- Bell, J. Bowyer. *A Time of Terror: How Democratic Societies Respond to Revolutionary Violence*. New York: Basic Book, 1978.
- Benes, Ross. "Porn Could Have a Bigger Economic Influence on the US than Netflix." *YahooFinance*, June 20, 2018. <https://finance.yahoo.com/news/porn-could-bigger-economic-influence-121524565.html>.
- Bennett, Bruce W. "Responding to Asymmetric Threats." Essay. In *New Challenges, New Tools for Defense Decisionmaking*. RAND Corporation, n.d.
- Bergen, Peter, David Sterman, Alyssa Sims, and Albert Ford, eds. "THE SEVERE THREAT TO EUROPE." JSTOR, 2016. <https://www.jstor.org/stable/resrep10494.7>.
- Berlin, Allan Hall in, and John Lichfield. "Germany Opens Its Gates: Berlin Says All Syrian Asylum-Seekers Are Welcome to Remain, as Britain Is Urged to Make a 'Similar Statement.'" *The Independent*, August 24, 2015. <https://www.independent.co.uk/news/world/europe/germany-opens-its-gates-berlin-says-all-syrian-asylum-seekers-are-welcome-to-remain-as-britain-is-10470062.html>.
- Bertram, Christopher. "Jean Jacques Rousseau." Stanford Encyclopedia of Philosophy. Stanford University, May 26, 2017. <https://plato.stanford.edu/entries/rousseau/>.
- Bilefsky, Dan, and Maïa De La Baume. "Terrorists Strike Charlie Hebdo Newspaper in Paris, Leaving 12 Dead." *NYTimes*, January 7, 2015. <https://www.nytimes.com/2015/01/08/world/europe/charlie-hebdo-paris-shooting.html>.
- Binetti, Ashley. "A New Frontier: Human Trafficking and ISIS's Recruitment of Women from the West", *Georgetown Institute for Women, Peace and Security*: (2015). <https://giwps.georgetown.edu/wp-content/uploads/2017/10/Human-Trafficking-and-ISISs-Recruitment-of-Women-from-the-West.pdf>.
- Birdwell, Jonathan, Chloe Colliver, Peter Pomerantsev, and Anne Applebaum. "Smearing Sweden: International Influence Campaign in the 2018 Swedish Election." London: Institue for Strategic Dialogue, 2018. Accessed August 8, 2020. <https://www.isdglobal.org/wp-content/uploads/2018/11/Smearing-Sweden.pdf>.
- Blake, Aaron. "A new study suggests fake news might have won Donald Trump the 2016 election." *The Washington Post*, April 3, 2018. Accessed August 8, 2020.

- <https://www.washingtonpost.com/news/the-fix/wp/2018/04/03/a-new-study-suggests-fake-news-might-have-won-donald-trump-the-2016-election/>.
- Blanchard, Christopher, and Carla Humud. (2018). "The Islamic State and U.S. Policy". *Fas.Org*. <https://fas.org/sgp/crs/mideast/R43612.pdf>.
- Blank, Stephen J. *Rethinking Asymmetric Threats*. Commonwealth Institute, 2003.
- Blumenthal-Barby, J.S. "Biases and heuristics in decision making and their impact on autonomy." *The American Journal of Bioethics* 16, no. 5 (2016): 5–15.
- Bogain, Ariane. "Security in the name of human rights: the discursive legitimization strategies of the war on terror in France". *Critical Studies on Terrorism* 10, no. 3 (2017): 476–500.
- Bond, Michael. *The Oxford Handbook of Chinese Psychology* (Oxford, UK: Oxford University Press, 2015), 32–67.
- Boot, Max. "Are we the Mongols of the Information Age?" *Los Angeles Times*, October 29, 2006. Accessed August 4, 2020. <https://www.latimes.com/archives/la-xpm-2006-oct-29-op-boot29-story.html>.
- Bornstein, Marc H. "Cultural Approaches to Parenting." *Parenting* 12, no. 2–3 (2012): 212–21. <https://doi.org/10.1080/15295192.2012.683359>.
- Borum, Randy. "Assessing Risk for Terrorism Involvement." *Journal of Threat Assessment and Management* 2, (2015): 63–87.
- Bowen, Becky Crookes Sue Elliott, F. Jeane Gerard, Mike Hellenbach, Helen Poole and Thanos Stamos, "The detection and policing of gun crime: Challenges to the effective policing of gun crime in Europe", *European Journal of Criminology*, vol.15(2) (2018).
- Bown, Chad P. "Export Controls: America's Other National Security Threat." *Duke Journal of Comparative & International Law*, 30 (2020): 283–308. Accessed August 1, 2020. <https://www.scholarship.law.duke.edu/djcil/vol30/iss2/4>.
- Boyd, Robert, and Peter J. Richerson. "Culture and the evolution of the human social instincts." *Roots of human sociality* (2006): 453–477.
- Brattberg, Erik, and Tim Maurer. "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks." *Carnegie Endowment for International Peace*, May 23, 2018. Accessed August 13, 2020. <https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435>.
- Brenan, Megan. "Americans Trust in Mass Media Edges Down to 41%." *Gallup*, September 26, 2019. Accessed August 8, 2020. <https://news.gallup.com/poll/267047/americans-trust-mass-media-edges-down.aspx>.

- Brinza, Andreea. "How Russia helped the United States fight Huawei in Central and Eastern Europe." *War on the Rocks*, March 12, 2020. Accessed July 25, 2020. <https://www.warontherocks.com/2020/03/how-russia-helped-the-united-states-fight-huawei-in-central-and-eastern-europe>.
- Brisard, Jean-Charles, and Damien Martinez. "Islamic State: the economy-based terrorist funding." Thomson Reuters 3 (2014). <http://www.gdr-elsj.eu/wp-content/uploads/2015/11/Islamic-State.pdf>.
- Brody, Howard et al. "U.S. responses to Japanese wartime inhuman experimentation after World War II." *Camb Q Healthc Ethics*, April 2014: 220–230. doi: 10.1017/S0963180113000753.
- Bronfenbrenner, Urie, Pamela A. Morris, William Damon, and Richard M. Lerner. "Handbook of child psychology." *The ecology of developmental process*. Wiley Publishers (2006).
- Brown, Joel S., John W. LaundrÃ©, and Mahesh Gurung. "The Ecology of Fear: Optimal Foraging, Game Theory, and Trophic Interactions." *Journal of Mammalogy* 80, no. 2 (1999): 385–99. Accessed August 23, 2020. doi:10.2307/1383287.
- Bryan-Low, Casell, Colin Packham, David Lague, Steve Stecklow and Jack Stubbs. "Hobbling Huawei: Inside the U.S. war on China's tech giant." *Reuters*, May 21, 2019. Accessed July 25, 2020. <https://www.reuters.com/investigates/special-report/huawei-usa-campaign>.
- Brzica, Nikola. "Understanding Contemporary Asymmetric Threats." *Croatian International Relations Review* 24, no. 83 (2018): 34–51. <https://doi.org/10.2478/cirr-2018-0013>.
- Bu, Ping. "A research report on Japanese use of chemical weapons during the Second World War." *Journal of Modern Chinese History*, vol. 2, June 2010: 155–172. <https://doi.org/10.1080/17535650701677239>.
- Buchanan, Ben. "The U.S. has AI Competition All Wrong." *Foreign Affairs*, August 7, 2020. Accessed August 7, 2020. <https://www.foreignaffairs.com/articles/united-states/2020-08-07/us-has-ai-competition-all-wrong>.
- Buckley, Edgar, and Ioan Mircea Pascu. "Article 5 and Strategic Reassurance." Washington DC: The Atlantic Council, 2010. Accessed August 14, 2020. www.jstor.org/stable/resrep03320.
- Buffaloe, David L. "Defining Asymmetric Warfare." Association of the United States Army, November 15, 2017. <https://www.ausa.org/publications/defining-asymmetric-warfare>.
- Bureau of International Security and Nonproliferation. *Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of*

- Bacteriological Methods of Warfare (Geneva Protocol)*, June 1925. Accessed August 13, 2020. <https://2009-2017.state.gov/t/isn/4784.htm#treaty>.
- Bureš, Oldrich. "EU Counterterrorism Policy: A Paper Tiger?". *e-International Relations*, August 22, 2013. Accessed August 24, 2020, <https://www.e-ir.info/2013/08/22/eu-counterterrorism-policy-a-paper-tiger/>.
- Buss, David M. *Evolutionary Psychology the New Science of the Mind*. New York City, NY: Routledge, 2019.
- Hendrickson, Noel. *Reasoning for Intelligence Analysts: A Multidimensional Approach of Traits, Techniques, and Targets*. New York: Rowman & Littlefield, 2018.
- Buss, David M. *Evolutionary Psychology: The New Science of the Mind (6th Edition)*. New York: Routledge, 2019.
- Byman, Daniel L. "Beyond Iraq and Syria: ISIS' Ability to Conduct Attacks Abroad." *Brookings*, June 8, 2017. <https://www.brookings.edu/testimonies/beyond-iraq-and-syria-isis-ability-to-conduct-attacks-abroad/>.
- Byrne, Richard, and Richard W. Byrne. *The thinking ape: Evolutionary origins of intelligence*. Oxford University Press on Demand, 1995.
- Callimachi, Rukmini. "ISIS Enshrines a Theology of Rape." *New York Times*, August 13, 2015. https://www.nytimes.com/2015/08/14/world/middleeast/isis-enshrines-a-theology-of-rape.html?_r=2.
- Cappacio, Tony and Jenny Leonard. "Huawei on List of 20 Chinese Companies that Pentagon Says Are Controlled by People's Liberation Army." *Time*, June 25, 2020. Accessed July 25, 2020. <https://time.com/5859119/huawei-chinese-military-company-list>.
- Carr, Madeline. "Public-private partnerships in national cyber-security strategies". *International Affairs*, Volume 92, Issue 1, January 2016. 43–62, <https://doi.org/10.1111/14682346.12504>.
- Carter, Ashton B., William J. Perry, and David Aidekman. "Countering Asymmetric Threats." *Belfer Center*, n.d., 1–10.
- Cavelty, Myiam Dunn. "The Politics of Cybersecurity: Balancing Different Roles of the State". *Center for Security Studies ETH Zurich*, 17 June 2019, css.ethz.ch/en/center/CSS-news/2019/06/the-politics-of-cybersecurity-balancing-different-roles-of-the-state-.html.
- Cavelty, Myriam Dunn. "The Militarization of Cyberspace: Why Less May Be Better." *2012 4th International Conference on Cyber Conflict*, Edited by C. Czosseck et al.
- Centre, UNESCO World Heritage. "Site of Palmyra." UNESCO World Heritage Centre, 2020. <https://whc.unesco.org/en/list/23/>.

- Cerulus, Laurens. "7 takeaways on the EU's Huawei plan." *Politico*, March 26, 2019. Accessed August 8, 2020. <https://www.politico.eu/article/europe-huawei-7-takeaways-on-plan>.
- Chandler, Adam. "German Mayoral Candidate Henriette Reker Wounded in Anti-Immigrant Attack." *The Atlantic*, October 17, 2015. <https://www.theatlantic.com/international/archive/2015/10/germany-cologne-mayor-attack-henriette-reker/411139/>.
- Chauzal, Grégory, Ko Colijn, Bibi van Ginkel, Christophe Paulussen and Sofia Zavagli. "Paris: 11/13/15 – Analysis and Policy Options". Policy Brief, *Clingendael Netherlands Institute for International Relations*, November 20, 2015. Accessed August 24, 2020, https://www.clingendael.org/sites/default/files/2017-06/Policy_Brief_Clingendael_ICCT-Paris111315Analysis_and_Policy_Options_November%202015_final.pdf
- Chen, Xinyin, Janet Chung, Rachel Lehcier-Kimel, and Doran French. "Culture and Social Development." *The Wiley-Blackwell Handbook of Childhood Social Development*, 2011, 141–60. <https://doi.org/10.1002/9781444390933.ch8>.
- Chen, Yuyu, and David Y. Yang. 2019. "The Impact of Media Censorship: 1984 or Brave New World?" *American Economic Review*, 109 (6): 2294–2332. doi: 10.1257/aer.20171765.
- Cheney, Dorothy L., and Robert M. Seyfarth. *How monkeys see the world: Inside the mind of another species*. University of Chicago Press, 2018.
- Chrisafis, Angelique. "The Guardian." *The Guardian*, January 12, 2015. <https://www.theguardian.com/world/2015/jan/12/-sp-charlie-hebdo-attackers-kids-france-radicalised-paris>.
- Clarke, Colin P. "Drugs & Thugs: Funding Terrorism through Narcotics Trafficking." *Journal of Strategic Security* 9, (2016): 1–15.
- Cleland, Jamie, and Ellis Cashmore. "Nothing Will Be the Same Again After the Stade de France Attack: Reflections of Association Football Fans on Terrorism, Security and Surveillance." *Journal of Sport and Social Issues* 42, no. 6 (December 2018): 454–69. doi:10.1177/0193723518797028.
- Cleveland, Charles T., Charles T. Connett, and Will Irwin. "Unconventional Warfare in the Gray Zone." *Joint Force Quarterly*. National Defense University Press, January 1, 2016. <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-80/Article/643108/unconventional-warfare-in-the-gray-zone/>.
- Clutton-Brock, T.H., P.H. Harvey, P.P.C. Bateson, and R.A. Hinde. "Growing points in ethology." (1976): 195–237. https://openlibrary.org/books/OL4880107M/Growing_points_in_ethology.

- Clutton-Brock, Tim H., ed. *Reproductive success: studies of individual variation in contrasting breeding systems*. University of Chicago Press, 1988.
- Coale, Ansley Johnson. *Growth and Structure of Human Populations: A Mathematical Investigation*. Princeton University Press, 2015.
- Coats, Daniel R. *Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, February 2018. Accessed August 16, 2020. <https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf>.
- Coats, Daniel R. *Worldwide Threat Assessment of the US Intelligence Community*, Senate Select Committee on Intelligence, January 2019. Accessed August 15, 2020. <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.
- Cohen, Dara Kay. *Rape during Civil War*. Ithaca, NY: Cornell University Press, 2016.
- Cole, Diane. "Study: What Was The Impact Of The Iconic Photo Of The Syrian Boy?", January 13, 2017. <https://www.npr.org/sections/goatsandsoda/2017/01/13/509650251/study-what-was-the-impact-of-the-iconic-photo-of-the-syrian-boy>.
- Conway, Maura. "Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research." *Studies in Conflict & Terrorism* 40, (2017): 77–98.
- Cook, Joana, and Gina Vale. *From Daesh to 'Diaspora': Tracing the Women and Minors of Islamic State*. London: International Centre for the Study of Radicalisation, 2018. https://icsr.info/wp-content/uploads/2018/07/Women-in-ISIS-report_20180719_web.pdf.
- Cordesman, Anthony H. "The Lessons and Challenges of September 2011 – the New '9/11.'" *The Lessons and Challenges of September 2011 – the New "9/11" | Center for Strategic and International Studies*. Center for Strategic and International Studies, August 14, 2020. <https://www.csis.org/analysis/lessons-and-challenges-september-2011-%E2%80%93-new-911>.
- Cosmides, Leda, and John Tooby. "Evolutionary psychology: A primer." (1997).
- Cosmides, Leda, and John Tooby. "From Evolution to Adaptations to Behavior: Toward an Integrated Evolutionary Psychology." In *Biological Perspectives on Motivated Activities*, edited by Roderick Wong, 10–74. Norwood, NJ: Ablex, 1995.
- Cosmides, Leda. "The logic of social exchange: Has natural selection shaped how humans reason? Studies with the Wason selection task." *Cognition* 31, no. 3 (1989): 187–276. <https://www.sciencedirect.com/science/article/pii/0010027789900231>.
- Costi, Alberto. "Complementary Approaches? A Brief Comparison of EU and United States Counter-Terrorism Strategies since 2001". *Victoria University of*

- Wellington Legal Research Papers* 22 (2019): 167–195. Accessed August 24, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3074136.
- Council of the European Union, *A European Security Strategy – A Secure Europe in a Better World*, European Communities, 2009. Accessed August 24, 2020, <https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf>.
- Council of the European Union, *Conclusions and plan of action of the extraordinary European Council meeting on 21 September 2001, SN 140/01*, September 21, 2001. Accessed August 24, 2020, <https://www.consilium.europa.eu/media/20972/140en.pdf>.
- Council of the European Union, *Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism*, November 28, 2008. Accessed August 24, 2020, <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32008F0919>.
- Council of the European Union, *Counter-terrorism strategy*, November 30, 2005. Accessed August 24, 2020, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A133275>.
- Council of the European Union, *Declaration on Combating Terrorism*, March 25, 2004. Accessed August 24, 2020, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/79637.pdf.
- Council of the European Union, *Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism*, May 19, 2014. Accessed August 24, 2020, <https://data.consilium.europa.eu/doc/document/ST-9956-2014-INIT/en/pdf>.
- Council of the European Union, *The European Union Strategy for Combating Radicalisation and Recruitment to Terrorism*, November 24, 2005. Accessed August 24, 2020, <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014781%202005%20REV%201>.
- Counter-Terrorism Committee Executive Directorate. *Identifying and Exploring the Nexus between Human Trafficking, Terrorism, and Terrorism Financing*. New York: United Nations Security Council, 2019. <https://www.un.org/sc/ctc/wp-content/uploads/2019/02/HT-terrorism-nexus-CTED-report.pdf>.
- Coyle, Diane, and Patrick Meier (2009). “New technologies in emergencies and conflicts: The role of information and social networks.” In *New Technologies in Emergencies and Conflicts: The Role of Information and Social Networks*. United Nations Foundation; Vodafone Foundation.
- Crisan, Magdalena. “Migration in the Kremlin’s Disinformation War.” *Bulletin of “Carol I” National Defence University* 8, no. 3 (September 2019): 7–13. Accessed August 8, 2020. ProQuest.

- Critical Infrastructure Sector Partnerships. 2019, April 23. Retrieved Accessed August 17, 2020, from <https://www.cisa.gov/critical-infrastructure-sector-partnerships>.
- Croft, Adrian and Apps, Peter. "NATO websites hit in cyber attack linked to Crimea tension.", <https://www.reuters.com/article/us-ukraine-nato-idUSBREA2E0T320140316>. Accessed August 17, 2020.
- Cross, Mai'a K. Davis. "Counter-terrorism in the EU's external relations". *Journal of European Integration* 39, no. 5 (2017): 609–624.
- Cummins, Denise Delarosa. "Social norms and other minds." *The evolution of mind* (1998): 30–50. <https://psycnet.apa.org/record/1998-06595-002>.
- Cummins, Denise Dellarosa. "Cheater detection is modified by social rank: The impact of dominance on the evolution of cognitive functions." *Evolution and human behavior* 20, no. 4 (1999): 229–248. <https://www.sciencedirect.com/science/article/pii/S1090513899000082>.
- Cummins, Denise Dellarosa. "Dominance hierarchies and the evolution of human reasoning." *Minds and Machines* 6, no. 4 (1996): 463–480. <https://link.springer.com/article/10.1007%2FBF00389654>.
- Cummins, Denise Dellarosa. "Evidence for the innateness of deontic reasoning." *Mind & Language* 11, no. 2 (1996): 160–190. <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-0017.1996.tb00039.x>.
- Cummins, Denise Dellarosa. "The evolutionary roots of intelligence and rationality." *Common Sense, Reasoning, and Rationality, Oxford UP, Oxford* (2002): 132–147.
- Ćurčić, Milica. "Asymmetric Threats in Security Studies." *Thematic Collection of Articles – Asymmetry and Strategy*, 2018, 17–29.
- Cyber Stratego: Strategic vs. Tactical Threat Intelligence. September, 2016. *Threat-Connect: Intelligence-Driven Security Operations*. Retrieved August 20, 2020, from <https://threatconnect.com/blog/strategic-vs-tactical-threat-intelligence/>.
- Daly, Martin, and Wilson, Margot. *Homicide*. Hawthorne, NY: Aldine, 1988.
- Damle, S. "Smart sugar? The sugar conspiracy." *Contemporary Clinical Dentistry* 8, no. 2 (2017): 191–191.
- Daniel E. Lieberman, *The Story of the Human Body: Evolution, Health, and Disease* (New York City, NY: Vintage Books, 2013), 25–48.
- Darden, Jessica Trisko. *Tackling Terrorists' Exploitation of Youth*. American Enterprise Institute, 2019. <https://www.aei.org/wp-content/uploads/2019/05/Tackling-Terrorists-Exploitation-of-Youth.pdf>.
- Darwin, Charles. *On the Origin of Species*. www.gutenberg.org. 6th ed. Accessed August 18, 2020. <http://www.gutenberg.org/files/2009/2009-h/2009-h.htm>.

- Datta, S. "Relative power and the acquisition of rank." *Primate social relationships* (1983). <https://ci.nii.ac.jp/naid/10015026754/>.
- David J. Epstein, *Range: Why Generalists Triumph in a Specialized World* (New York City, NY: Riverhead Books, 2019), 25–26.
- Defending Democracy Together. *The Russia Tweets*, n.d. Accessed August 9, 2020. <https://russiatweets.com/>.
- Denardis, L., and A.M. Hackl. "Internet Governance by Social Media Platforms." *Telecommunications Policy* 39, no. 9 (October 2015): 761–70. <https://doi.org/10.1016/j.telpol.2015.04.003>.
- Department of Biochemistry and Molecular Biophysics Thomas Jessell, Steven Siegelbaum, and A.J. Hudspeth. *Principles of neural science*. Edited by Eric R. Kandel, James H. Schwartz, and Thomas M. Jessell. Vol. 4. New York: McGraw-hill, 2000.
- Department of Justice. "Joint Terrorism Task Force Charges Three Men Who Allegedly Sought To Exploit Protests In Las Vegas And Incite Violence, U.S. Attorney's Office, District of Nevada. Published 3 June 2020; accessed 16 August 2020. <https://www.justice.gov/usao-nv/pr/joint-terrorism-task-force-charges-three-men-who-allegedly-sought-exploit-protests-las>.
- Deutsche Welle. "AfD: What You Need to Know about Germany's Far-Right Party | DW | 28.10.2019." DW.COM. Accessed August 30, 2020. <https://www.dw.com/en/afd-what-you-need-to-know-about-germanys-far-right-party/a-37208199>.
- Deutsche Welle. "Germany: More than 1,600 Crimes 'targeted Refugees and Asylum-Seekers' | DW | 27.03.2020." DW.COM. Accessed August 30, 2020. <https://www.dw.com/en/germany-more-than-1600-crimes-targeted-refugees-and-asylum-seekers/a-52935715>.
- Deutsche Welle. "Man Who Stabbed Mayor of Cologne Sentenced to 14 Years in Jail | DW | 01.07.2016." DW.COM. Accessed August 29, 2020. <https://www.dw.com/en/man-who-stabbed-mayor-of-cologne-sentenced-to-14-years-in-jail/a-19371698>.
- Devlin, Kat. "Unlike in US, Most European Students Learn a Foreign Language", Pew Research Center (Pew Research Center, August 6, 2018), <https://www.pewresearch.org/fact-tank/2018/08/06/most-european-students-are-learning-a-foreign-language-in-school-while-americans-lag/>.
- Dewsbury, Donald A. "Dominance rank, copulatory behavior, and differential reproduction." *The Quarterly Review of Biology* 57, no. 2 (1982): 135–159. <https://www.journals.uchicago.edu/doi/abs/10.1086/412672>.
- Diana Munoz Robino, *Global Destination Cities Index 2019* (Mastercard, 2019).

- DiGiacomo, Richard J. "Prostitution as a Possible Funding Mechanism for Terrorism." MA Thesis, Naval Postgraduate School, 2010.
- Disinformation: A case study of the 2018 Swedish national elections." PhD diss., Swedish Defence University, 2019. 2019. Accessed August 4, 2020. <http://www.diva-portal.org/smash/get/diva2:1324745/FULLTEXT01.pdf>.
- Dobson, GB, A. Rege, and KM Carley. "Informing Active Cyber Defense with Realistic Adversarial Behaviour." *Journal of Information Warfare* 17, no. 2 (2018): 16–31. Accessed August 6, 2020. doi:10.2307/26633151.
- Doise, Willem, and Joaquim Pires Valentin. "Levels of Analysis in Social Psychology." In *International Encyclopedia of the Social & Behavioral Sciences*, edited by James D. Wright, 899–903. Oxford: Elsevier, 2015. <https://doi.org/10.1016/B978-0-08-097086-8.24032-4>.
- Doxsee, Catrina, Nicholas Harrington and Seth G. Jones, "The Tactics and Targets of Domestic Terrorists", Center for Strategic and International Studies, July 2020.
- Ducaru, Sorin. "NATO advances in its new operational domain: cyberspace." Fifth Domain, July 5, 2018. Accessed August 11, 2020. <https://www.fifthdomain.com/opinion/2018/07/05/nato-advances-in-its-new-operational-domain-cyberspace/>.
- Dulay, Heidi C., and Marina K. Burt. "Natural sequences in child second language acquisition." *Language learning* 24, no. 1 (1974): 37–53.
- Dworkin, Anthony. "Europe's New Counter-Terror Wars". Policy Brief, *European Council on Foreign Relations*, October 2016. Accessed August 24, 2020, https://www.ecfr.eu/page/-/ECFR192_-_EUROPES_NEW_COUNTER-TERROR_WARS_FINAL.pdf.
- Dymont, Jen. "The Cyber Attribution Dilemma: 3 Barriers to Cyber Deterrence." Security Intelligence, December 28, 2018, accessed August 17, 2020, <https://securityintelligence.com/the-cyber-attribution-dilemma-3-barriers-to-cyber-deterrence/>.
- Edwards, Benjamin, Alexander Furnas, Stephanie Forrest, and Robert Axelrod. "Strategic Aspects of Cyberattack, Attribution, and Blame." *Proceedings of the National Academy of Sciences of the United States of America* 114, no. 11 (2017): 2825–830. Accessed August 17, 2020. doi:10.2307/26480254.
- Ellis, Lee. "Dominance and reproductive success among nonhuman animals: a cross-species comparison." *Ethology and sociobiology* 16, no. 4 (1995): 257–333. <https://www.sciencedirect.com/science/article/pii/016230959500050U>.
- El-Masri, Samar. "Prosecuting ISIS for the Sexual Slavery of the Yazidi Women and Girls." *The International Journal of Human Rights* 22, (2018): 1047–1066.

- Embassy of France in Washington, *Press conference given by M. François Hollande, President of the Republic* (excerpts), Paris, February 5, 2015, published on February 9, 2015. Accessed August 24, 2020, <https://fr.franceintheus.org/spip.php?article6498>.
- Emergent Effects of a Wired World*, 109–49. New Brunswick, New Jersey; London: Rutgers University Press, 2011. Accessed August 14, 2020. www.jstor.org/stable/j.ctt5hjgfh.8.
- Esper, Mark T., U.S. Secretary of Defense. “As Prepared Remarks by Secretary of Defense Mark T. Esper at the Munich Security Conference.” U.S. Department of Defense, February 15, 2020. Accessed August 15, 2020. <https://defense.gov/Newsroom/Speeches/Speech/Article/2085577/as-prepared-remarks-by-secretary-of-defense-mark-t-esper-at-the-munich-security>.
- European Commission. “Commission Recommendation – Cybersecurity of 5G networks”, March 26, 2019. Accessed August 1, 2020. <https://www.ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks>.
- Evan Osnos, New Yorker. Accessed August 17, 2020. <https://www.cfr.org/backgrounder/media-censorship-china>.
- Evans, Robert, and Josh Wilson. “The Boogaloo Movement Is Not What You Think.” Bellingcat. Published 27 May 2020; accessed 16 August 2020. <https://www.bellingcat.com/news/2020/05/27/the-boogaloo-movement-is-not-what-you-think/>.
- Evon, Dan. “Were These Mexican Police Officers Brutalized by Members of a Migrant Caravan?” *Snopes*, October 22, 2018. Accessed August 17, 2020. <https://www.snopes.com/fact-check/mexican-police-caravan-photos/>.
- Fan, L. “On contradiction in cognition development: A personal view.” In *Issues in cognition: Proceedings of a joint conference in psychology*. Washington, DC: National Academy of Sciences, American Psychological Association. 1984.
- Farivar, Cyrus, and Cerf, Vinton G. “Estonia”, in *The Internet of Elsewhere: The Emergent Effects of a Wired World*, (New Brunswick, New Jersey; London: Rutgers University Press, 2011), 109–49. www.jstor.org/stable/j.ctt5hjgfh.8.
- FBI Counterterrorism Division, *White Supremacist Recruitment of Military Personnel since 9/11*, Published 7 July 2008; accessed 10 August 2020, <https://documents.law.yale.edu/sites/default/files/White%20Supremacist%20Recruitment%20of%20Military%20Personnel%20Since%209-11-ocr.pdf>.
- Federal Bureau of Investigation. “Remembering Pan Am Flight 103”, December 14, 2018. <https://www.fbi.gov/news/stories/remembering-pan-am-flight-103-30-years-later-121418>.

- Federation of American Scientists. "Chemical Weapons." Accessed August 15, 2020.
- Federation of American Scientists. "Iranian NBC Policy, Capabilities, and Employment Options." Denial and Jeopardy: Deterring Iranian Use of NBC Weapons. Accessed August 16, 2020. <https://fas.org/nuke/guide/iran/doctrine/dajd/ch5.html>.
- Fedigan, Linda Marie. "Dominance and reproductive success in primates." *American Journal of Physical Anthropology* 26, no. S1 (1983): 91–129. <https://onlinelibrary.wiley.com/doi/abs/10.1002/ajpa.1330260506>.
- Fehr, Ernst, and Urs Fischbacher. "The Nature of Human Altruism." *Nature* 425, no. 6960 (2003): 785–91. <https://doi.org/10.1038/nature02043>.
- Felbab-Brown, Vanda. "Stuck in the Middle: Iraq and the Enduring Conflict between United States and Iran." Brookings. Brookings Institute, January 29, 2020. <https://www.brookings.edu/blog/order-from-chaos/2020/01/29/stuck-in-the-middle-iraq-and-the-enduring-conflict-between-united-states-and-iran/>.
- Feng, Emily. "The Latest U.S. Blow to China's Huawei Could Knock Out Its Global 5G Plans." *NPR*, May 28, 2020. Accessed July 27, 2020. <https://www.npr.org/2020/05/28/862658646/the-latest-u-s-blow-to-chinas-huawei-could-knock-out-its-global-5g-plans>.
- Fenrick, William J. "The Rule of Proportionality and Protocol in Conventional Warfare." *Hein Online*, 1982, 91.
- Ferris, Izzy. "Men with Histories of Sexual Violence are 'More Likely to Be Terrorists' so Police Should Monitor Them, Top Lawyer Claims." *Daily Mail*, May 26, 2019. <https://www.dailymail.co.uk/news/article-7073493/Men-histories-sexual-violence-likely-terrorists-lawyer-claims.html>.
- Financial Times. "France's National Front Taps into Rising Anti-Immigrant Mood", September 6, 2015. <https://www.ft.com/content/62131206-5473-11e5-8642-453585f2cfd>.
- Fishman, Edward and Siddharth Mohandas. "A Council of Democracies Can Save Multilateralism." *Foreign Affairs*, August 3, 2020. Accessed August 3, 2020. <https://foreignaffairs.com/articles/asia/2020-08-03/council-democracies-can-save-multilateralism>.
- Flichy, Patrice. "The Birth of Long Distance Communication. Semaphore Telegraphs in Europe." *Réseaux. The French Journal of Communication*, 1.1 (1993): 81–101. Accessed August 9, 2020. https://www.persee.fr/doc/reso_0969-9864_1993_num_1_1_3272.
- Fortin, Jacey. "The Statue at the Center of Charlottesville's Storm." *The New York Times*. Published 13 August 2017; accessed 17 August 2020. <https://www.nytimes.com/2017/08/13/us/charlottesville-rally-protest-statue.html>.

- Freeman, Michael. "The Sources of Terrorist Financing: Theory and Typology." *Studies in Conflict & Terrorism* 34, (2011): 461–475.
- Frischknecht, Friedrich. "The history of biological warfare." *EMBO Rep*, June 2003: S47–S52. doi: 10.1038/sj.embor.embor849.
- Furedi, Frank. "Lost for Words". *The Guardian*, January 17, 2008. Accessed on August 24, 2020, <https://www.theguardian.com/commentisfree/2008/jan/17/lostforwords>.
- Gadagkar, Raghavendra. "Chapter: 4 The Biotechnology Revolution: Exploring New Territory Together." *Sciences Engineering Medicine*, 2016. Accessed August 14, 2020. <https://www.nap.edu/read/21810/chapter/7>.
- Galbert, Simond de. "After the Paris Attacks, France Turns to Europe in its Time of Need". Commentary, *Center for Strategic and International Studies* (2015). Accessed August 24, 2020, www.csis.org/analysis/after-paris-attacks-france-turns-europe-its-time-need.
- Ganesan, K., S.K. Raza, and R. Vijayaraghavan. "Chemical Warfare Agents." *J Pharm Bioallied Sci*, Jul-Sep 2010: 166–178. doi: 10.4103/0975-7406.68498.
- Gardner, Frank. "Germany Shooting: 'Far-right extremist' carried out shisha bars attack", BBC, August 14th, 2020. <https://www.bbc.com/news/world-europe-51567971>.
- Gartrell, Nate and Fiona Kelliher, "Santa Cruz deputy's alleged killer charged with assassinating federal cop in Oakland ambush; authorities link attacks to extremist group that believes civil war looming." Santa Cruz Sentinel. Published 16 June 2020; accessed 17 August 2020, <https://www.santacruzsentinel.com/2020/06/16/santa-cruz-deputys-alleged-killer-charged-with-assassinating-federal-cop-in-oakland-ambush/>.
- Gates, Scott, and Sukanya Podder. "Social media, recruitment, allegiance and the Islamic State." *Perspectives on Terrorism* 9, no. 4 (2015): 107–116.
- Gaughan, Anthony J. "Illiberal Democracy: The Toxic Mix of Fake News, Hyperpolarization, and Partisan Election Administration." *Duke Journal of Constitutional Law & Public Policy* 12, no. 3 (2017): 57–139. Accessed August 13, 2020. <https://scholarship.law.duke.edu/djclpp/vol12/iss3/3>.
- Gazzaniga, Michael S., Leda Cosmides, and John Tooby. "Social Exchange: The Evolutionary Design of a Neurocognitive System." In *The Cognitive Neurosciences*, 1295–1308. Cambridge, MA: MIT Press, 2004. <https://psycnet.apa.org/record/2005-01373-087>.
- Gedmin, Jeffrey. "Right-Wing Populism in Germany: Muslims and Minorities after the 2015 Refugee Crisis." Brookings, July 24, 2019. <https://www.brookings>.

- edu/research/right-wing-populism-in-germany-muslims-and-minorities-after-the-2015-refugee-crisis/.
- George Soros, *The Crisis of Global Capitalism: Open Society Endangered* (New York: PublicAffairs, 1998).
- Georgy, Michael. "Captive Islamic State Militant Says Mass Rapes Were 'Normal'." *Reuters*, February 17, 2017. <https://www.reuters.com/article/us-mideast-crisis-mosul-prisoners-idUSKBN15W1N0>.
- Gigerenzer, Gerd, and Klaus Hug. "Domain-specific reasoning: Social contracts, cheating, and perspective change." *Cognition* 43, no. 2 (1992): 127–171. <https://www.sciencedirect.com/science/article/pii/001002779290060U>.
- Gilli, Andrea. "NATO & 5G: what strategic lessons?", *NATO Defense College*, no. 13 (July 2020): 1–6. Accessed August 6, 2020. <https://www.jstor.org/stable/resrep25095>.
- Global Terrorism Index 2019 – Measuring the Impact of Terrorism*, Institute for Economics & Peace. Accessed August 24, 2020, <https://www.economicsandpeace.org/wp-content/uploads/2020/08/GTI-2019web.pdf>.
- Goebel, Greg. "A History of Chemical & Biological Warfare." Accessed August 11, 2020. https://www.cia.gov/library/abbottabad-compound/65/65A3FAC0A645BA2C3FAC8C187499C16D_the_history_of_chemical_war_fare.pdf.
- Golbeck, Jennifer. 2019. "Benford's Law Can Detect Malicious Social Bots". *First Monday* 24 (8). <https://doi.org/10.5210/fm.v24i8.10163>.
- Golovchenko PhD, Yevgeniy. "Using Social Network Analysis to Understand Disinformation on Social Media." Sage Publications Ltd, 2019. Accessed August 7, 2020. doi:10.4135/9781526498632.
- Gonzales, Richard. "For 7th Consecutive Year, Visa Overstays Exceed Illegal Border Crossings." *NPR*, January 16, 2019. Accessed August 13, 2020. <https://www.npr.org/2019/01/16/686056668/for-seventh-consecutive-year-visa-overstays-exceeded-illegal-border-crossings>.
- Goodman, Elisa Mala, J. David. "At Least 80 Dead in Norway Shooting." *NYTimes*, July 22, 2011. <https://www.nytimes.com/2011/07/23/world/europe/23oslo.html>.
- Gottschall, Jonathan. "Explaining Wartime Rape." *The Journal of Sex Research* 41, (May 2004): 129–136.
- Goudeau, Jessica. "Refugee Resettlement is Close to Collapse. That Was Trump's Plan." *The New York Times* online, July 28, 2020. Accessed August 13, 2020. <https://www.nytimes.com/2020/07/28/opinion/us-refugee-resettlement-trump.html>.
- Government Accountability Office, *The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report*, June 26, 2009.

- Graff, Garret M. "Could Trump Win the War on Huawei—and Is Tik Tok Next?", July 14, 2020. Accessed July 25, 2020. <https://www.wired.com/story/could-trump-win-the-war-on-huawei-and-is-tiktok-next>.
- Gramlich, John and Katherine Schaeffer, "7 facts about guns in the U.S.", Pew Research Center, accessed August 10th, 2020. <https://www.pewresearch.org/fact-tank/2019/10/22/facts-about-guns-in-united-states/>.
- Grant Wardlaw, "Political Terrorism: Theory, tactics, and counter-measures", Cambridge University Press, (1982): 39.
- Gray, Rosie. "Trump Declines to Affirm NATO's Article 5." *The Atlantic*. May 25, 2017.
- Greene, Alan. "Defining Terrorism: One Size Fits All?" *International and Comparative Law Quarterly* 66, (April 2017): 411–440. <https://doi.org/10.1017/S0020589317000070>.
- Gressel, Gustav. "Russia's Hybrid Interference in Germany's Refugee Policy." ECFR. European Council on Foreign Relations, February 4, 2016. https://www.ecfr.eu/article/commentary_russias_hybrid_interference_in_germanys_refugee_policy5084.
- Greven, Thomas. "The rise of right-wing populism in Europe and the United States." *Friederich-Ebert-Stiftung* (2016): 1–8. Accessed August 8, 2020. https://www.fesdc.org/fileadmin/user_upload/publications/RightwingPopulism.pdf.
- Grier, David Alan. "What the Count of Monte Cristo Can Teach Us About Cybersecurity." *IEEE Spectrum*, January 25, 2018. Accessed August 17, 2020. <https://spectrum.ieee.org/techtalk/telecom/security/what-the-count-of-monte-cristo-can-teach-us-about-cybersecurity>.
- Grip, Lina and John Hart. *The use of chemical weapons in the 1935–36 Italo-Ethiopian War*. SIPRI Arms Control and Non-proliferation Programme, October 2009. Accessed August 8, 2020. <https://www.sipri.org/sites/default/files/Italo-Ethiopian-war.pdf>
- Guest, Kenneth J. *Cultural Anthropology: A Toolkit for a Global Age*. New York, NY: W.W. Norton & Company, 2014. 40
- Guo, S., Feng, G. Understanding Support for Internet Censorship in China: An Elaboration of the Theory of Reasoned Action. *Journal of Chinese Political Science* 17, 33–52 (2012). <https://doi.org/10.1007/s11366-011-9177-8>
- Hacal, Sarah, "30 years after the fall of the Berlin wall, right-wing extremism is on the rise as the East lags behind", abc News, accessed August 7th, 2020. <https://abcnews.go.com/International/30-years-fall-berlin-wall-wing-extremism-rise/story?id=66670250>

- Hahn-Holbrook, Jennifer, Colin Holbrook, and Jesse Bering. "Snakes, spiders, strangers: How the evolved fear of strangers may misdirect efforts to protect children from harm." *Protecting children from violence: Evidence-based interventions* 26 (2010): 3–289.
- Haig, Alexander M. "Chemical Warfare in Southeast Asia and Afghanistan." United States Department of State, 1982. Accessed August 11, 2020. <https://www.cia.gov/library/readingroom/docs/CIA-RDP97M00248R000500010018-6.pdf>.
- Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53, no. 4 (2009): 1155–175. Accessed August 6, 2020. www.jstor.org/stable/27735139.
- Harcourt, Alexander H. "Alliances in contests and social intelligence." (1988). <https://psycnet.apa.org/record/1988-98392-011>.
- Harris, Paul L., and María Núntez. "Understanding of permission rules by pre-school children." *Child development* 67, no. 4 (1996): 1572–1591. <https://srcd.onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-8624.1996.tb01815.x>.
- Haselton, Martie G., Daniel Nettle, and Damian R. Murray. "The Evolution of Cognitive Bias." *The Handbook of Evolutionary Psychology*, 2015, 1–20. <https://doi.org/10.1002/9781119125563.evpsych241>.
- Hashim, Ahmed Salah. "State and Non-State Hybrid Warfare." Oxford Research Group, May 21, 2018. <https://www.oxfordresearchgroup.org.uk/blog/state-and-non-state-hybrid-warfare>.
- Hebb, Donald Olding. *The organization of behavior: a neuropsychological theory*. J. Wiley; Chapman & Hall, 1949.
- Hendrickson, Noel. *Reasoning for Intelligence Analysis: A Multidimensional Approach of Traits, Techniques, and Targets* (New York City, NY: Rowan and Littlefield, 2018), 26–27.
- Herculano-Houzel, Suzana. "The human brain in numbers: a linearly scaled-up primate brain." *Frontiers in human neuroscience* (2009): 31.
- Hermida PhD, Alfred. "Alfred Hermida Discusses Social Networks and Misinformation." SAGE Publications Ltd, 2019. Accessed August 7, 2020. doi: 10.4135/9781526492210.
- Herring, MJ, and KD Willett. "Active Cyber Defense: A Vision for Real-Time Cyber Defense." *Journal of Information Warfare* 13, no. 2 (2014): 46–55. Accessed July 31, 2020. www.jstor.org/stable/26487121.
- Herta, Laura-Maria. "Hybrid Warfare – A Form of Asymmetric Conflict." *International conference KNOWLEDGE-BASED ORGANIZATION* 23, no. 1 (July 20, 2017): 135–43. <https://doi.org/10.1515/kbo-2017-0021>.

- Hertzberg, Hendrik. "War and Words". *The New Yorker*, February 6, 2006. Accessed on August 24, 2020, <https://www.newyorker.com/magazine/2006/02/13/war-and-words>.
- Heuer, Richards J. *Psychology of Intelligence Analysis*. Washington, DC: Central Intelligence Agency, 1999.
- Heuser, Beatrice. *Reading Clausewitz*. London: Pimlico, 2002.
- Hill, Jonah, Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers (May 20, 2012). Berkman Center Research Paper, Harvard Belfer Center for Science and International Affairs Working Paper, Available at SSRN: <https://ssrn.com/abstract=2439486>.
- Hills, Jill. *The Struggle for Control of Global Communication*. University of Illinois Press, 2002. Accessed August 6, 2020. <https://www.jstor.org/stable/10.5406/j.ctt2ttcks.13>.
- Hoffman, Adonis. "Facial Recognition Could Stop Terrorists before They Act | The Hill." *The Hill*, March 9, 2020. <https://thehill.com/opinion/technology/486570-facial-recognition-could-stop-terrorists-before-they-act>.
- Hoffman, Bruce. "A Counterterrorism Strategy for the Obama Administration". *Terrorism and Political Violence* 21, no. 3 (2009): 359–377.
- Hoffman, Bruce. *Inside Terrorism: Revised and Expanded Edition*. New York: Columbia University Press, 2006.
- Hoffman, David E. "Cracking open the Soviet biological weapons system, 1990." The National Security Archive, 2009. Accessed August 12, 2020. <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB315/index.htm>
- Hopp, Toby, Patrick Ferrucci, and Chris J. Vargo. "Why Do People Share Ideologically Extreme, False, and Misleading Content on Social Media? A Self-Report and Trace Data–Based Analysis of Countermedia Content Dissemination on Facebook and Twitter." *Human Communication Research* (May 2020): 1–28. Accessed August 9, 2020. <https://doi.org/10.1093/hcr/hqz022>.
- Horneman, A. (2019, September 09). Situational Awareness for Cybersecurity: An Introduction. Retrieved August 07, 2020, from https://insights.sei.cmu.edu/sei_blog/2019/09/situational-awareness-for-cybersecurity-an-introduction.html.
- Horowitz, Ami. "Stockholm Syndrome." YouTube video, 10:18. December 12, 2016. Accessed August 14, 2020. <https://www.youtube.com/watch?v=RqalgeQXQgl>.
- Howard, Michael. "What's in a name? How to fight terrorism". *Foreign Affairs* (January/February 2002).

- Hubbard, Ben. "Germany Takes Rare Step in Putting Syrian Officers on Trial in Torture Case." *The New York Times*, April 23, 2020. <https://www.nytimes.com/2020/04/23/world/middleeast/syria-germany-war-crimes-trial.html>.
- Hussain, Murtaza. (2020). "Islamic State's Goal: "Eliminating The Grayzone" Of Co-existence Between Muslims And The West". *The Intercept*. <https://theintercept.com/2015/11/17/islamic-states-goal-eliminating-the-grayzone-of-coexistence-between-muslims-and-the-west/>.
- Hyde, Janet. "Gender Differences in Aggression." In *The Psychology of Gender: Advances through Meta-analysis*, edited by J.S. Hyde and M.C. Linn 67-101. Baltimore: Johns Hopkins University Press, 1986.
- Ilves, Toomas Hendrik. "The Consequences of Cyber Attacks", *Journal of International Affairs* 70, no. 1 (2016): 175–81, accessed August 14, 2020, www.jstor.org/stable/90012601.
- Institute for Economics & Peace. Global Terrorism Index 2019: Measuring the Impact of Terrorism, Sydney, November 2019. Available from: <http://visionofhumanity.org/reports> (accessed August 12th, 2020).
- International Committee of the Red Cross. "Rule 93. Rape and Other forms of Sexual Violence." Accessed November 23, 2020. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule93.
- Iran Watch. "A History of Iran's Chemical Weapon-Related Efforts." Wisconsin Project on Nuclear Arms Control, November 2019. Accessed August 16, 2020. <https://www.iranwatch.org/our-publications/weapon-program-background-report/history-irans-chemical-weapon-related-efforts>.
- Ivanov, Iskren, and Velizar Shalamanov. "NATO and Partner Countries Cooperation in Countering Asymmetric and Hybrid Threats in South Eastern Europe's Cyberspace." *Towards Effective Cyber Defense in Accordance with the Rules of Law* 149 (2020): 59–70.
- Jacobson, Michael. "Terrorist Financing and the Internet." *Studies in Conflict & Terrorism* 33, (2010): 353–363.
- Jakarta Globe. "Europe's Refugee Blockade", February 23, 2016. <https://jakarta-globe.id/multimedia/europes-refugee-blockade/>.
- James, William. *The Principles of Psychology*. Vol. 1. Cosimo, Inc., 2007.
- Janda, Jakub. "The Lisa Case STRATCOM Lessons for European States." *Security Policy Working Paper No.11/2016* (January 1, 2016): 1/4.
- Jian, He. "Huawei and the Creation of China's Orwellian Surveillance State." *The Epoch Times*, December 24, 2018, updated January 8, 2019. Accessed July 25, 2020. https://www.theepochtimes.com/huawei-and-the-creation-of-chinas-orwellian-surveillance-state_2747922.html.

- John Hopkins Bloomberg School of Public Health. "Preparedness Home: Biological Weapons." Accessed August 6, 2020. https://www.jhsph.edu/research/centers-and-institutes/johns-hopkins-center-for-public-health-preparedness/tips/topics/Biologic_Weapons/BioWeapons.html.
- Johnson, James A. "The New Generation of Isolationists." *Foreign Affairs* 49, no. 1 (1970): 136. <https://doi.org/10.2307/20037824>.
- Johnson, Rob. "Analytical Culture in the U.S. Intelligence Community: An Ethnographic Study", Central Intelligence Agency (Central Intelligence Agency, June 28, 2008), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/chapter_1.htm, 4.
- Johnston, Rob. *Analytic Culture in the US Intelligence Community: An Ethnographic Study*. Washington, D.C., DC: Center for the Study of Intelligence, Central Intelligence Agency, 2005.
- Joseph Patrick Henrich, *The Secret of Our Success: How Culture Is Driving Human Evolution, Domesticating Our Species, and Making Us Smarter* (Princeton, NJ: Princeton University Press, 2016).
- Jospeph, Anthony. "Fingerprints Reveal 2 of the Paris Suicide Bombers Entered Europe through Greece." Daily Mail, November 21, 2015. <https://www.dailymail.co.uk/news/article-3327928/Fingerprints-reveal-TWO-Paris-suicide-bombers-entered-Europe-Greece-month-attacks.html>.
- Journal of Economic Perspectives* 31, no. 2 (April 2017): 211–235. Accessed August 10, 2020. <https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211>.
- Kagan, Robert. "Power and Weakness". *Policy Review* 113, (June/July 2002).
- Kan, Paul Rexton, and J. Boone Bartholomees. "Lawyers, Guns, and Money: Transnational Threats and U.S. National Security". Strategic Studies Institute, US Army War College, 2010, pp. 207–214, The U.S. Army War College Guide to National Security Issues, www.jstor.org/stable/resrep12024.17. Accessed 5 Aug. 2020.
- Kania, Elsa. "Innovation in the New Era of Chinese Military Power." The Diplomat. The Diplomat, July 25, 2019. <https://thediplomat.com/2019/07/innovation-in-the-new-era-of-chinese-military-power/>.
- Kasapoglu, Can. "Cyber Security: Understanding the Fifth Domain." Istanbul: Centre for.
- Kasapoglu, Can. "Cyber Security: Understanding the Fifth Domain". Istanbul: Centre for Economics and Foreign Policy Studies, 2017. Accessed August 11, 2020. www.jstor.org/stable/resrep14048.

- Katherine Pherson and Randolph Pherson, *Critical Thinking for Strategic Intelligence*, 2nd ed. (Thousand Oaks, CA: CQ Press, 2017), 89.
- Kathleen Kitao and Kenji Kitao, *An Analysis of Japanese University Entrance Exams Using Corpus-Based Tools*, 2008, <http://www.j-let.org/~wcf/proceedings/d-053.pdf>.
- Kazeem B. Ajide & Ibrahim D. Raheem (2020) Does Democracy Really Fuel Terrorism in Africa?, *International Economic Journal*, 34:2, 297–316, DOI: 10.1080/10168737.2020.1741014.
- Kennedy, John F. *A Nation of Immigrants*. New York: Harper Perennial, 2008.
- Kim, Hyun-Kyung, Elizabeth Philipp, and Hattie Chung. "North Korea's Biological Weapons Program: The Known and Unknown. *HARVARD Kennedy School, Belfer Center for Science and International Affairs*, October 2017. <https://www.belfercenter.org/sites/default/files/2017-10/North%20Korea%20Biological%20Weapons%20Program.pdf>.
- Kimball, Daryl G. "The Chemical Weapons Convention (CWC) at a Glance." Arms Control Association, April 2020. Accessed August 13, 2020. <https://www.armscontrol.org/factsheets/cwcglance>.
- Kirby, Emma Jean. "The city getting rich from fake news." *BBC*, December 5, 2016. Accessed August 8, 2020. <https://www.bbc.com/news/magazine-38168281>.
- Koblentz, Gregory D. "Chemical-weapon use in Syria: atrocities, attribution, and accountability." *The Nonproliferation Review*, vol. 26, February 2020: 575–598. <https://doi.org/10.1080/10736700.2019.1718336>.
- Koh, B.C. "The Recruitment of Higher Civil Servants in Japan: A Comparative Perspective." *Asian Survey* 25, no. 3 (1985): 292–309. Accessed August 18, 2020. doi:10.2307/2644120.
- Kravchenko, Alexander V. "How Humberto Maturana's biology of cognition can revive the language sciences." *Constructivist Foundations* 6, no. 3 (2011): 352–362.
- Krikorian, Lena. "Islamisation of Europe: Myth or Reality? – Polemics." Polemics, March 1, 2018. <http://www.polemics-magazine.com/dasicon2018/islamisation-europe-myth-reality>.
- Kruglanski, Arie W., and Shira Fishman. "Terrorism between Syndrome and Tool." *Current Directions in Psychological Science* 15, (2006): 45–48.
- Kurdi, Abdulrahman Abdulkadir. "The Islamic State." London: Mansell (2016).
- Kuru, Huseyin. "Evolution of War and Cyber-Attacks in the Concept of Conventional Warfare." *Journal of Learning and Teaching in Digital Age*, 2018, 12–20.
- Kuzio, Taras, and Paul D'Anieri. "Annexation and Hybrid Warfare in Crimea and Eastern Ukraine." *E-International Relations*, July 5, 2018. <https://www.e-ir>.

- info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/.
- Lachow, Irving. Report. Center for a New American Security, 2013. Accessed July 31, 2020. www.jstor.org/stable/resrep06088.
- Lafrance, Adrienne. "How the 'Fake News' Crisis of 1896 Explains Trump." *The Atlantic*, January 19, 2017. Accessed August 13, 2020. <https://www.theatlantic.com/technology/archive/2017/01/the-fake-news-crisis-120-years-ago/513710/>.
- Lalumière, Martin L., Grant T. Harris, Vernon L. Quinsey, and Marnie E. Rice. *The Causes of Rape: Understanding Individual Differences in Male Propensity for Sexual Aggression*. Washington D.C.: American Psychological Association, 2005.
- Landon-Murray, Michael, and Stephen Coulthart. "Intelligence Studies Programs as US Public Policy: a Survey of IC CAE Grant Recipients." *Intelligence and National Security* 35, no. 2 (2019): 269–82. <https://doi.org/10.1080/02684527.2019.1703487>.
- Laurenco, Marco and Louis Marinos. "ENISA Threat Landscape for 5G Networks", *European Union Agency for Cybersecurity*, (November 2019). Accessed August 1, 2020. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>.
- Le'onard, Sarah. "Border Controls as a Dimension of the European Union's Counter-Terrorism Policy: A Critical Assessment." *Intelligence and National Security* 30, no. 2–3 (2015): 306–332.
- Leggeri, Fabrice, ed. "Foreword." Accessed September 2, 2020. <https://frontex.europa.eu/about-frontex/foreword/>.
- Lemay, A., S. Knight, and JM Fernandez. "Intelligence Preparation of the Cyber Environment (IPCE): Finding the High Ground in Cyberspace." *Journal of Information Warfare* 13, no. 3 (2014): 46–56. Accessed July 31, 2020. www.jstor.org/stable/26487107.
- Lété, Bruno. *NATO and the EU: The Essential Partners*. Report. Edited by Lindstrom Gustav and Tardy Thierry. NATO Defense College, 2019. 33–44. Accessed August 11, 2020. <https://www.ndc.nato.int/news/news.php?icode=1352>.
- Levitt, Matthew. "Terrorist financing and the Islamic state." testimony submitted to the House Committee on Financial Services 13 (2014).
- Lewis, Brian C. "Information Warfare." *Federation of American Scientists*. Accessed August 17, 2020. <https://fas.org/irp/eprint/snyder/infowarfare.htm>.
- Lewis, James Lewis. "Can Telephones Race? 5G and the Evolution of Telecom Part I." *Center for Strategic International Studies*, 2020. Accessed July 25, 2020. <https://www.jstor.org/stable/resrep24786>.

- Lian, Yi-Zheng. "Where Spying is the Law." *The New York Times*, March 13, 2019. Accessed August 23, 2020. <https://www.nytimes.com/2019/03/13/opinion/china-canada-huawei-spying-espionage-5g.html>.
- Lichtblau, Eric. "Hate Crimes Against American Muslims Most Since Post-9/11 Era." *New York Times*, September 17, 2016. Accessed August 9, 2020. <https://www.nytimes.com/2016/09/18/us/politics/hate-crimes-american-muslims-rise.html>.
- Liddle, James R., Lance S. Bush, and Todd K. Shackelford. "An Introduction to Evolutionary Psychology and Its Application to Suicide Terrorism." *Behavioral Sciences of Terrorism and Political Aggression* 3, (2011): 176–197.
- Lieberman, Daniel E., Brandeis M. McBratney, and Gail Krovitz. "The evolution and development of cranial form in Homo sapiens." *Proceedings of the National Academy of Sciences* 99, no. 3 (2002): 1134–1139.
- Liggett, Roberta. "Exploring Online Sextortion." *Family & Intimate Partner Violent Quarterly* 11, (2019): 45–56.
- Lim, Darren J. and Victor Ferguson. "Conscious Decoupling: The Technology Security Dilemma." In *China Dreams*, edited by Jane Golley, Linda Javin, Ben Hillman, Sharon Strange, 119–131 (ANU Press, 2020). Accessed July 25, 2020. <https://jstor.org/stable/j.ctv12sdxmk.15>.
- Lindell, Jordan. "Clausewitz: War, Peace and Politics." *E-International Relations*, November 26, 2009. <https://www.e-ir.info/2009/11/26/clausewitz-war-peace-and-politics/>.
- Lindkvist, Hugo. "He filmed the police interview that Trump saw: the material was not edited ethically." *Dagens Nyheter*, February 23, 2017. Accessed August 13, 2020. <https://www.dn.se/kultur-noje/he-filmed-the-police-interview-that-trump-saw-the-material-was-not-edited-ethically/>.
- Lowenthal, Mark. *Intelligence: From Secrets to Policy*, 8th ed. (Thousand Oaks, CA: SAGE/CQ Press, 2020), 441–499.
- Lykins, Amy D., ed. *Encyclopedia of Sexuality and Gender*. Springer Nature Switzerland AG, 2020. <https://doi.org/10.1007/978-3-319-59531-3>.
- Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs* 89, no. 5 (2010): 97–108. Accessed July 31, 2020. www.jstor.org/stable/20788647.
- MacKenzie, Alexander. "The European Union's Increasing Role in Foreign Policy Counterterrorism". *Journal of Contemporary European Research* 6, no. 2 (2010): 147–163. Accessed August 24, 2020, <http://www.jcer.net/ojs/index.php/jcer/article/view/269/214>.

- Maiese, Michelle. "Moral or Value Conflicts." *Beyond Intractability*. Eds. Guy Burgess and Heidi Burgess. Conflict Information Consortium, University of Colorado, Boulder. Posted: July 2003.
- Maizland, Lindsay and Andrew Chatzky. "Huawei: China's Controversial Tech Giant." *Council on Foreign Relations*, August 6, 2020. Accessed August 23, 2020. <https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant>.
- Majoran, Andrew. "The Illusion of War: Is Terrorism A Criminal Act or an Act of War?" *The Mackenzie Institute*, August 1, 2014. <https://mackenzieinstitute.com/2014/08/the-illusion-of-war-is-terrorism-a-criminal-act-or-an-act-of-war/>.
- Malamuth, Neil M. and Eldad Z. Malamuth. "Integrating Multiple Levels of Scientific Analysis and the Confluence Model of Sexual Coercers." *Jurimetrics* 39, (1999): 157–179.
- Malet, David. *Foreign fighters: Transnational identity in civil conflicts*. Oxford University Press, (2013).
- Malik, Nikita. "Human Trafficking Continues to Be Used by Terrorists: The ICC Must Address It." *Forbes*, June 20, 2019. <https://www.forbes.com/sites/nikitamalik/2019/06/20/human-trafficking-continues-to-be-used-by-terrorists-the-icc-must-address-it/?sh=352e018d230b>.
- Malik, Nikita. "Trafficking Terror: How Modern Slavery and Sexual Violence Fund Terrorism." London: The Henry Jackson Society, 2017. <https://henryjackson-society.org/wp-content/uploads/2017/10/HJS-Trafficking-Terror-Report-web.pdf>.
- Maniszewska, Katarzyna. *Pionierzy Terroryzmu Europejskiego: Frakcja Czerwonej Armii*. Kraków: Apeiron, 2014.
- Mansfield, David. "Denying Revenue or Wasting Money? Assessing the Impact of the Air Campaign Against 'Drugs Labs' in Afghanistan." London: London School of Economics and Political Science, April 2019. <https://www.lse.ac.uk/united-states/Assets/Documents/mansfield-april-update.pdf>.
- Manuel, Anja Manuel and Kathleen Hicks. "Can China's Military win the Tech War? How the United States Should-and Should Not-Counter Beijing's Civil-Military Fusion." *Foreign Affairs*, July 29, 2020. Accessed July 29, 2020. <https://www.foreignaffairs.com/articles/united-states/2020-07-29/can-chinas-military-win-tech-war>.
- Marchi, Regina. "With Facebook, Blogs, and Fake News, Teens Reject Journalistic 'Objectivity.'" *Journal of Communication Inquiry* 36, no. 3 (July 2012): 246–62. Accessed August 7, 2020. doi:10.1177/0196859912458700.

- Marrin, Stephen, and Jonathan D. Clemente. "Modeling an Intelligence Analysis Profession on Medicine1." *International Journal of Intelligence and CounterIntelligence* 19, no. 4 (2006): 642–65. <https://doi.org/10.1080/08850600600829882>.
- Marrin, Stephen. "Intelligence Analysis: Structured Methods or Intuition?" *American Intelligence Journal* 25, no. 1 (2007): 7–16. Accessed August 18, 2020. www.jstor.org/stable/44327067.
- Marrin, Stephen. "CIA's Kent School: Improving Training for New Analysts." *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (2003): 609–37. <https://doi.org/10.1080/716100469>.
- Marrin, Stephen. "Training and Educating U.S. Intelligence Analysts." *International Journal of Intelligence and CounterIntelligence* 22, no. 1 (2008): 131–46. <https://doi.org/10.1080/08850600802486986>.
- Matthews, Earl D., Harold J. Arata, and Brian L. Hale. "Cyber Situational Awareness." *The Cyber Defense Review* 1, no. 1 (2016): 35–46. Accessed August 12, 2020. www.jstor.org/stable/26267298.
- Mauroni, Albert J. *Eliminating Syria's Chemical Weapons*. US Air Force Center for Unconventional Weapons Studies, Future Warfare Series, No. 58. June 2017. Accessed August 16, 2020. <https://media.defense.gov/2019/Apr/11/2002115522/-1/-1/0/58ELIMINATINGSYRIACW.PDF>.
- Max Roser, Hannah Ritchie and Esteban Ortiz-Ospina (2015) – "Internet". *Published online at OurWorldInData.org*. Retrieved from: '<https://ourworldindata.org/internet>'.
- McCaskill, Noland D. "Trump promises wall and massive deportation program." *Politico*, August 31, 2016. Accessed August 13, 2020. <https://www.politico.com/story/2016/08/donald-trump-immigration-address-arizona-227612>.
- McDonald, Melissa M., Carlos D. Navarrete, and Mark Van Vugt. "Evolution and the Psychology of Intergroup Conflict: The Male Warrior Hypothesis." *Philosophical Transactions of the Royal Society B: Biological Sciences* 367, (2012): 670–679.
- McGeehan, Timothy P. "Countering Russian Disinformation. (21st Century Political Warfare)." *Parameters* 48, no. 1 (March 2018): 49–57. Accessed August 13, 2020. <https://www.hsdl.org/?view&did=812849>.
- McGranahan, Carole. "An anthropology of lying: Trump and the political sociability of moral outrage." *American Ethnologist*, 44, no. 2 (2017): 243–248. Accessed September 21, 2020. <https://doi.org/10.1111/amet.12475>.

- McKibbin, William F., Todd K. Shackelford, Aaron T. Goetz, and Valerie G. Starratt. "Why Do Men Rape? An Evolutionary Psychological Perspective." *Review of General Psychology* 12, (2008): 86–97.
- Mekhennet, Souad, and Joby Warrick. 2020. "The Appeal Of ISIS Fades Among Europeans Who Returned Home From Syria". *The Washington Post*. https://www.washingtonpost.com/national-security/the-appeal-of-isis-fades-among-europeans-who-returned-home-from-syria/2020/06/14/754b3e0e-acb9-11ea-9063-e69bd6520940_story.html.
- Merloe, Patrick. "Election Monitoring Vs. Disinformation. (Authoritarianism Goes Global)." *Journal of Democracy* 26, no. 3 (July 2015): 79–93. Accessed August 8, 2020. doi:10.1353/jod.2015.0053.
- Mersky, J.P., J. Topitzes, and Arthur J. Reynolds. "Impacts of adverse childhood experiences on health, mental health, and substance use in early adulthood: A cohort study of an urban, minority sample in the US." *Child abuse & neglect* 37, no. 11 (2013): 917–925.
- Meserve, Stephen A., and Daniel Pemstein. "Google Politics: The Political Determinants of Internet Censorship in Democracies." *Political Science Research and Methods* 6, no. 2 (2017): 245–63. <https://doi.org/10.1017/psrm.2017.1>.
- Microsoft Corp v United States Department of Justice et al in the United States District Court, Western District of Washington, No. 2:16-cv-00537.
- Miller, James N., and Michael O'Hanlon. "Quality over Quantity: U.S. Military Strategy and Spending in the Trump Years." *Foreign Policy at Brookings*, January 2019, 1–9.
- Mitchell, Anna and Larry Diamond. "China's Surveillance State Should Scare Everyone." *The Atlantic*, February 2, 2018. Accessed July 18, 2020. <https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203>.
- Mitchell, Robert W. "The psychology of human deception." *Social Research* (1996): 819–861. <https://www.jstor.org/stable/40972317>.
- Mogherini, Federica and Sir Julian King. "Navigating the internal-external security nexus". *EU Security and Defence in a Volatile World, European Political Strategy Centre* (2017). Accessed August 24, 2020, <https://medium.com/eu-security-and-defence-in-a-volatile-world/navigating-the-internal-external-security-nexus-1dcdd213f380>.
- Monar, Jörg. "The EU as an International Counter-terrorism Actor : Progress and Constraints". *Intelligence and National Security* 30, no. 2–3 (2015): 333–356.
- Moodie, Michael. "The Soviet Union, Russia, and the Biological and Toxin Weapons Convention." *The Nonproliferation Review/Spring* 2001, Accessed

- August 13, 2020. <https://www.nonproliferation.org/wp-content/uploads/npr/81moodie.pdf>.
- Moore, Jack. "New Analysis Shows ISIS Fighters Originate From 70 Countries." *Newsweek*, April 20, 2016. <https://www.newsweek.com/new-analysis-shows-isis-fighters-originate-70-countries-449968>.
- Mosely, Alexander. "The Philosophy of War." Internet Encyclopedia of Philosophy. Accessed August 24, 2020. <https://iep.utm.edu/war/>.
- Mueller, John. "Is There Still a Terrorist Threat?: The Myth of the Omnipresent Enemy". *Foreign Affairs* (September/October 2006). Accessed August 24, 2020, <https://www.foreignaffairs.com/articles/2006-09-01/there-still-terrorist-threat-myth-omnipresent-enemy>.
- Mueller, Milton. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. New York, NY: John Wiley & Sons, 2017. <https://doi.org/9781509501250>.
- NATO. "1990: Summary." Last modified August 23, 2001. Accessed August 11, 2020. <https://www.nato.int/docu/update/1990/summarye.htm>.
- NATO. "Brussels Summit Declaration." Last modified August 30, 2018. Accessed August 14, 2020. https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20.
- NATO. "Collective defense – Article 5." Last modified November 25, 2019. Accessed August 17, 2020. https://www.nato.int/cps/en/natohq/topics_110496.htm#:~:text=Article%20%20provides%20that%20if,to%20assist%20the%20Ally%20attacked.
- NATO. "Cyber defense." Last modified March 17, 2020. Accessed August 14, 2020, https://www.nato.int/cps/en/natohq/topics_78170.htm.
- NATO. "Member countries." Last modified March 24, 2020. Accessed August 14, 2020, https://www.nato.int/cps/en/natohq/topics_52044.htm.
- NATO. "NATO will defend itself." Last modified August 29, 2019. Accessed August 11, 2020. https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en.
- NATO. "Prague Summit Declaration." Last modified May 6, 2014. Accessed 11 August, 2020. https://www.nato.int/cps/en/natohq/official_texts_19552.htm?
- NATO. "Statement by the North Atlantic Council concerning malicious cyber activities." Last modified June 3, 2020. Accessed August 11, 2020. https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en.
- NATO. "The North Atlantic Treaty." Last modified April 10, 2019. Accessed August 11, 2020. https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

- NATO. "The North Atlantic Treaty." NATO. North Atlantic Treaty Organization, April 1, 2009. https://www.nato.int/cps/en/natolive/official_texts_17120.htm.
- Nehring, Christopher. "Umbrella or pen? The murder of Georgi Markov. New facts and old questions." *Journal of Intelligence History*, February 2016: 47–58. <https://doi.org/10.1080/16161262.2016.1258248>.
- Nesser, Petter. "Military Interventions, Jihadi Networks, and Terrorist Entrepreneurs: How the Islamic State Terror Wave Rose So High in Europe." *CTC Sentinel* 12, no. 3 (2019).
- News, BBC. "Brussels Fatal Gun Attack at Jewish Museum." BBC News, May 24, 2014. <https://www.bbc.com/news/world-europe-27558918>.
- Noack, Rick. "Sweden has no idea what Trump meant when he said, 'You look at what's happening...in Sweden.'" *The Washington Post*, February 19, 2017. Accessed August 13, 2020. <https://www.washingtonpost.com/news/world-views/wp/2017/02/19/sweden-has-no-idea-what-trump-meant-when-he-said-you-look-at-whats-happening-in-sweden/>.
- Nolen, Elizabeth. "Female Suicide Bombers: Coerced or Committed?" *Global Security Studies* 7, (Spring 2016): 30–40.
- Nonproliferation Review/Spring*, 2001, Accessed August 11, 2020. <https://www.nonproliferation.org/wp-content/uploads/npr/81ali.pdf>
- Noor, Sitara. "Cyber (In) Security: A Challenge to Reckon With." *Strategic Studies* 34, no. 2/3 (2014): 1–19. Accessed August 12, 2020. doi:10.2307/48527537.
- NRA-ILA. *nd*. "State Gun Laws". Accessed August 11th, 2020. <https://www.nraila.org/gun-laws/state-gun-laws/>.
- Nuclear Threat Initiative. "Australia Group (GA)." Accessed August 14, 2020. <https://www.nti.org/learn/treaties-and-regimes/australia-group-ag/>.
- Nuclear Threat Initiative. "Countries: China." Accessed August 16, 2020. <https://www.nti.org/learn/countries/china/chemical/>.
- Nuclear Threat Initiative. "Countries: Iran: Biological." Accessed August 16, 2020. <https://www.nti.org/learn/countries/iran/biological/>.
- Nuclear Threat Initiative. "Countries: Iran: Chemical." Accessed August 16, 2020. <https://www.nti.org/learn/countries/iran/chemical/>.
- Nunziato, Dawn Carla, *Misinformation Mayhem: Social Media Platforms' Efforts to Combat Medical and Political Misinformation* (2020). 19 First Amendment L. Rev. ____ (2020), GWU Legal Studies Research Paper No. 2020–48, GWU Law School Public Law Research Paper No. 2020–48, Available at SSRN: <https://ssrn.com/abstract=3672257>.
- O'Malley, Roberta Liggett and Karen M. Holt. "Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime." *Journal of*

- Interpersonal Violence* online first, (2020): 1–26. <https://doi-org.huaryu.kl.oakland.edu/10.1177/0886260520909186>.
- Obar, Jonathan A., and Steven S. Wildman. "Social Media Definition and the Governance Challenge – An Introduction to the Special Issue." *SSRN Electronic Journal* 39, no. 9 (October 2015): 745–810. <https://doi.org/10.2139/ssrn.2663153>.
- Obert, Jonathan and Elias Schultz, "Right Wing Militias, Guns, and the Technics of State Power", *Law, Culture, and the Humanities*, vol. 16(2), 2017.
- O'Brien, Danny. "China's Global Reach: Surveillance and Censorship Beyond the Great Firewall." Electronic Frontier Foundation, December 29, 2019. <https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall>.
- OECD. "Inflows of asylum seekers." OECD International Migration Database and labour market outcomes of immigrants. Accessed September 21, 2020. <http://www.oecd.org/els/mig/keystat.htm>.
- OPCW News. "OPCW Marks Completion of Destruction of Russian Chemical Weapons Stockpile." October 2017. Accessed August 15, 2020. <https://www.opcw.org/media-centre/news/2017/10/opcw-marks-completion-destruction-russian-chemical-weapons-stockpile>.
- Oppong, Steward Harrison. "Human Trafficking through Organized Crime." *International Journal of Humanities and Social Science* 2, (October 2012): 37–43.
- Orkaby, Asher. "Forgotten Gas Attacks in Yemen Haunt Syria Crisis." Accessed August 11, 2020. <https://wcfia.harvard.edu/publications/forgotten-gas-attacks-yemen-haunt-syria-crisis>.
- Pacini, Rosemary, and Seymour Epstein. "The Relation of Rational and Experiential Information Processing Styles to Personality, Basic Beliefs, and the Ratio-Bias Phenomenon." *Journal of Personality and Social Psychology* 76, no. 6 (1999): 972–87. <https://doi.org/10.1037/0022-3514.76.6.972>.
- Pannier, Alice and Olivier Schmitt. "To fight another day: France between the fight against terrorism and future warfare". *International Affairs* 95, no. 4 (2019): 897–916.
- Parachini, John V. "North Korea's CBW Program: How to Contend with Imperfectly Understood Capabilities." RAND Santa Monica United States. Accessed August 16, 2020. <https://apps.dtic.mil/sti/pdfs/AD1056014.pdf>.
- Parkin, William and Brent Klein, Jeff Gruenewald, Joshua Freilich, and Steven Chermak, "Threats of violent Islamist and far-right extremism: What does the research say?" National Consortium for the Study of Terrorism and Responses

- to Terrorism. Published 17 February 2017; accessed 17 August 2020. <https://www.start.umd.edu/news/threats-violent-islamist-and-far-right-extremism-what-does-research-say>.
- Parrington, Alan J. "Mutually Assured Destruction Revisited." *Airpower Journal*, 1997, 4–19.
- Pellerin, Cheryl. "Lynn: cyberspace is new domain of warfare." Armed Forces Press Service, CENTCOM, October 19, 2010. Accessed August 15, 2020. <https://centcom.mil/MEDIA/NEWSARTICLES/News-Article-View/Article/884164/lyn-cyberspace-is-new-domain-of-warfare>.
- Permanent Mission of France to the United Nations in New York, *François Hollande's Speech Before a Joint Session of Parliament*, November 16, 2015. Accessed August 24, 2020, <https://onu.delegfrance.org/Francois-Hollande-s-Speech-Before-a-Joint-Session-of-Parliament>.
- Perper, Rosie. 2020. "ISIS Made Millions From Taxes That It Then Used To Run Garbage Collections And Even A DMV". *Business Insider*. <https://www.businessinsider.com/islamic-state-used-taxes-to-grow-power-and-offer-services-2018-4>.
- Persian Gulf War Illnesses Task Force. "Intelligence Update: Chemical Warfare Agent Issues During the Persian Gulf War." April 2002. Accessed August 11, 2020. <https://www.hsdl.org/?view&did=2796>.
- Petras, George. "'Daesh,' Other Islamic State Names Explained." *USA Today*, November, 17, 2015. <https://www.usatoday.com/story/news/world/2015/11/17/islamic-state-names/75889934/>.
- Pew Research Center, Global Attitudes Project. "Number of Refugees to Europe Surges to Record 1.3 Million in 2015", August 2, 2016. <https://www.pewresearch.org/global/2016/08/02/number-of-refugees-to-europe-surges-to-record-1-3-million-in-2015/>.
- Pick, Hella. "NATO seeks a new role." *The Guardian*. May 18, 1990. <https://www.newspapers.com/image/260321413/>.
- Pickard, Victor W., and David Elliot Berman. *After Net Neutrality: a New Deal for the Digital Age*. New Haven: Yale University Press, 2019.
- Pompeo, Michael R., U.S. Secretary of State. "The Tide is Turning Toward Trusted 5G Vendors." U.S. Department of State, June 24, 2020. Accessed July 25, 2020. <https://www.state.gov/the-tide-is-turning-toward-trusted-5g-vendors>.
- Pompeo, Michael R., U.S. Secretary of State. "The United States Protects National Security and the Integrity of 5G Networks." U.S. Department of State, May 15, 2020. Accessed July 25, 2020. <https://www.state.gov/>

- the-united-states-protects-the-national-security-and-the-integrity-of-5g-networks.
- Porter, Eduardo and Karl Russell. "Migrants Are on the Rise Around the World, and Myths About Them Are Shaping Attitudes." *The New York Times*, June 20, 2018. Accessed August 15, 2020. <https://www.nytimes.com/interactive/2018/06/20/business/economy/immigration-economic-impact.html>.
- Potts, Malcolm and Thomas Hayden. *Sex and War: How Biology Explains Warfare and Terrorism and Offers a Path to a Safer World*. Dallas: BenBella Books, 2008.
- Price, M. (2016). Freedom vs. Security. *InterMedia*, 44 (3), 9–11. Retrieved from https://repository.upenn.edu/asc_papers/675.
- Price, Michelle L. and Scott Sonner. "Army reservist, Navy and Air Force vets plotted to terrorize Vegas protests, prosecutors charge." *Military Times*. Published 4 June 2020; accessed 16 August 2020. <https://www.militarytimes.com/news/your-military/2020/06/04/army-reservist-navy-and-air-force-vets-plotted-to-terrorize-vegas-protests-prosecutors-charge/>.
- Puente, Antonio E., Maria Sol Mora, and Juan Manuel Munoz-Cespedes. "Neuropsychological assessment of Spanish-speaking children and youth." In *Handbook of clinical child neuropsychology*, pp. 371–383. Springer, Boston, MA, 1997.
- Putin, Vladimir. "Being strong: National security guarantees for Russia." *Rossiiskaya Gazeta*, February 2012. Accessed August 15, 2020. <http://archive.premier.gov.ru/eng/events/news/18185/>.
- Ravndal, Jacob Aasland, "Explaining right-wing terrorism and violence in Western Europe: Grievances, opportunities and polarization", *European Journal of Political Research*, 15 (2018).
- Reality Check team, "Are Migrants Driving Crime in Germany?" *BBC News*, September 13, 2018. <https://www.bbc.com/news/world-europe-45419466#:~:text=In%202014%2C%20German%20men%20between,seekers%20who%20came%20in%202015.>
- Reference to Biological Weapons Capabilities." *Journal of Defence Studies*, 2015: 131–156. Accessed August 16, 2020. https://idsa.in/system/files/jds/jds_9_2_2015_DanyShoham.pdf.
- Rehbein, David. "An Open Letter to Homeland Security on 'Rightwing Extremists'." *Fox News*. Published 14 April 2009; accessed 10 August 2020. <https://www.foxnews.com/opinion/an-open-letter-to-homeland-security-on-rightwing-extremists>.

- Reporters Without Borders. "WORLDWIDE ROUND-UP of journalists killed, detained, held hostage, or missing in 2018." 2019.
- Repucci, Sarah. "Media Freedom: A Downward Spiral." *Freedom House*, 2019. Accessed August 7, 2020. <https://freedomhouse.org/report/freedom-and-media/2019/media-freedom-downward-spiral>.
- Reuters*. March 15, 2014. Accessed August 14, 2020. <https://www.reuters.com/article/us-ukraine-nato/nato-websites-hit-in-cyber-attack-linked-to-crimea-tension-idUSBREA2E0T320140316>.
- Richerson, Peter J., Robert Boyd, and Joseph Henrich. "Gene-culture coevolution in the age of genomics." *Proceedings of the National Academy of Sciences* 107, no. Supplement 2 (2010): 8985–8992.
- Riding, Alan, ed. "EXPLOSION KILLS 4 AND INJURES MANY ON TRAIN IN PARIS." *NYTimes*, July 26, 1995. <https://www.nytimes.com/1995/07/26/world/explosion-kills-4-and-injures-many-on-train-in-paris.html>.
- Rieker, Pernille. "Editor's Introduction". *Security Dialogue. Special Section: European Security and Transatlantic Relations in the Age of International Terrorism: Challenges for the Nordic Countries* 36, no. 3 (September 2005): 395–396.
- Riikonen, Ainikki. "Decide, Disrupt, Destroy." *Strategic Studies Quarterly*, 13, no. 4, (Winter 2019): 122–145. Accessed July 25, 2020. <https://www.jstor.org/stable/10.2307/26815049>.
- Rissanen, Jenni. "The Biological Weapons Convention." Nuclear Threat Initiative, March 2003. Accessed August 13, 2020. <https://www.nti.org/analysis/articles/biological-weapons-convention/>.
- Risse, Thomas, Börzel Tanja A., and Anke Draude. *The Oxford Handbook of Governance and Limited Statehood*, 2018.
- Rogoff, Barbara. *The cultural nature of human development*. Oxford university press, 2003.
- Róisín Áine Costello, *Law, Policy and the Internet (International Journal of Law and Information Technology*, 2019), 204–207.
- Rose, Michel. "French Parties Scramble to Halt Rise of Far-Right National Front." *Reuters*, December 7, 2015. <https://www.reuters.com/article/us-france-politics/french-parties-scramble-to-halt-rise-of-far-right-national-front-idUSKBN0TQ0T820151207>.
- Rosenau, William. "The Dark History of America's First Female Terrorist Group." *Politico*, May 3, 2020. <https://www.politico.com/news/magazine/2020/05/03/us-history-first-women-terrorist-group-191037>.

- Ross, Andrew S and Damian J Rivers. "Discursive Deflection: Accusation of 'Fake News' and the Spread of Mis- and Disinformation in the Tweets of President Trump." *Social Media + Society* (April 2018): 1–12. Accessed August 10, 2020. doi:10.1177/2056305118776010.
- Roy, Muhammad Iqbal. "The Global Counter-Terrorism Strategies". *Journal of Politics and International Studies* 5, no. 1 (2019): 25–40. Accessed August 24, 2020, http://pu.edu.pk/images/journal/politicsAndInternational/PDF/3_v5_1_2019.pdf.
- Russell, Alison Lawlor, "Cyber Attacks on Estonia", In *Cyber Blockades*. Washington, DC: Georgetown University Press, 2014. 69–95, www.jstor.org/stable/j.ctt9qdsfj.9.
- Sahill, Pamir H. "The U.S. War on Terror Discourse". *Insight Turkey. A New Scramble for Africa? The Role of Great and Emerging Powers*, 21, no.1 (2019): 189–210.
- Sahl, Jason W. et al. "A *Bacillus anthracis* Genome Sequence from the Sverdlovsk 1979 Autopsy Specimens. Accessed August 12, 2020. <https://mbio.asm.org/content/7/5/e01501-16>.
- Saito, Yoshitaka. "Consequences of high stakes testing on the family and schools in Japan." *KEDI Journal of Educational Policy* 3, no. 1 (2006).
- Sanger, David A. and Mary K. Brooks. "Battlefield 5G: Are the U.S. and China destined for a forever-war over network control?" *Wilson Quarterly* (Spring 2020). Accessed August 22, 2020. <https://www.wilsonquarterly.com/who-writes-the-rules/battlefield-5g/> (2/11).
- Sapolsky, Robert M., *Behave: The Biology of Humans At Our Best and Worst*. New York, New York: Penguin Press, 2017.
- Sarker, Md Nazirul Islam, Md Altab Hossin, Xiaohua Yin, and Md Kamruzzaman Sarkar. "One Belt One Road initiative of China: Implication for future of global development." *Modern Economy* 9, no. 4 (2018): 623–638.
- Satariano, Adam, Stephen Castle and David E. Sanger. "U.K. Bars Huawei for 5G as Tech Battle Between China and the West Escalates." *The New York Times*, July 14, 2020. Accessed August 17, 2020. <https://www.nytimes.com/2020/07/14/business/huawei-uk-5g.html>.
- Savage, Chet R., and Craig T. Palmer. "Sexual Access as a Benefit of War." In *Encyclopedia of Evolutionary Psychological Science*, edited by Todd K. Shackelford and Viviana A. Weekes-Shackelford. Springer, Cham, 2016. https://doi.org/10.1007/978-3-319-16999-6_965-1.
- Schindler, Hans-Jakob, and Frederique Gautier. "Looting and Smuggling of Artifacts as a Strategy to Finance Terrorism Global Sanctions as a Disruptive and

- Preventive Tool." *International Journal of Cultural Property* 26, no. 3 (2019): 331–42. doi:10.1017/S0940739119000225.
- Schmid, Alex. "Terrorism – The Definitional Problem". *Case Western Reserve Journal of International Law* 36 (2004): 375–419. Accessed August 24, 2020, <https://scholarlycommons.law.case.edu/jil/vol36/iss2/8>.
- Schmitt, Michael N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, 2017. doi: 10.1017/9781316822524.
- Schofield, Hugh. "How Napoleon's semaphore telegraph changed the world." *BBC News Magazine*, June 17, 2013. Accessed August 15, 2020. <https://www.bbc.com/news/magazine-22909590>.
- Schuurman, Bart, Lasse Lindekilde, Stefan Malthaner, Francis O'Connor, Paul Gill, and Noémie Bouhana. "End of the Lone Wolf: The Typology that Should Not Have Been." *Studies in Conflict & Terrorism* 42, (2019): 771–778.
- Sey, A., Coward, C., Bar, F., Sciadas, G., Rothschild, C., & Koepke, L. (2013). Connecting people for development: Why public access ICTs matter. Seattle: Technology & Social Change Group, University of Washington Information School.
- Seyfarth, Robert M., and Dorothy L. Cheney. "Grooming, alliances and reciprocal altruism in vervet monkeys." *Nature* 308, no. 5959 (1984): 541–543. <https://www.nature.com/articles/308541a0>.
- Shah, Saqib, Liz Thomas and Cat Weeks. "Europe lacks a unified approach to Huawei despite yearlong assessments." *S&P Global Market Intelligence*, July 27, 2020. Accessed August 8, 2020. <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/europe-lacks-unified-approach-to-huawei-despite-yearlong-assessments-59602291>.
- Shahbaz, Adrian, and Allie Funk. "The Crisis of Social Media", 2019. <https://freedomhouse.org/report/freedom-net/2019/crisis-social-media>.
- Shapiro, Ari. "The Current State Of ISIS As Its End Draws Near." NPR. NPR, February 19, 2019. <https://www.npr.org/2019/02/19/696075305/the-current-state-of-isis-as-its-end-draws-near>.
- Shapiro, Jeremy. "Where You Stand Depends on Where You Get Hit: US and European Counterterrorism Strategies". *Security Studies Seminar*, November 9, 2005, Brookings Institution. Accessed August 24, 2020, http://web.mit.edu/SSP/seminars/wed_archives05fall/shapiro.htm.
- Shearlaw, Maeve. "Did the #bringbackourgirls Campaign Make a Difference in Nigeria?" *The Guardian*, April 14, 2015. <https://www.theguardian.com/world/2015/apr/14/nigeria-bringbackourgirls-campaign-one-year-on>.

- Sheinis, Daniel. "The Links Between Human Trafficking, Organized Crime, and Terrorism." *American Intelligence Journal* 30, no. 1 (2012): 68–77. Accessed August 11, 2020. www.jstor.org/stable/26201986.
- Sherwood, Harriet. "The Guardian." *the Guardian*, May 5, 2019. <https://www.theguardian.com/technology/2019/may/05/airbnb-homelessness-renting-housing-accommodation-social-policy-cities-travel-leisure>.
- Shoham, Dany. "China's Biological Warfare Programme: An Integrative Study with Special." *Special*.
- Sidell, Frederick R., Ernest T. Takafuji, and David R. Franz. *Medical Aspects of Chemical and Biological Warfare*. Office of the Surgeon General, Department of the Army, United States of America, 1997. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.8260&rep=rep1&type=pdf#page=24>.
- Silverman, Craig. "This Analysis Shows How Viral Fake Election News Stories Outperformed Real News on Facebook." *BuzzFeed News*, November 16, 2016. Accessed August 13, 2020. <https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook>.
- Sinnott, Richard. "*Public Opinion and the New Security Environment*". European Union Institute for Security Studies (EUISS), 1997, European Public Opinion and Security Policy, www.jstor.org/stable/resrep06994.5. Accessed 5 Aug. 2020.
- Skodo, Admir. "Sweden: By Turns Welcoming and Restrictive in its Immigration Policy." *Migration Policy Institute*, December 6, 2018. Accessed August 13, 2020. <https://www.migrationpolicy.org/article/sweden-turns-welcoming-and-restrictive-its-immigration-policy>.
- Solis, Jonathan A., and Philip D. Waggoner. 2020. "Measuring Media Freedom: An Item Response Theory Analysis of Existing Indicators." *British Journal of Political Science*. Cambridge University Press, 1–20. doi:10.1017/S0007123420000101.
- Song, Ray. Publication. *The Hermit Threat : A Historical Analysis of Cyberwarfare, Its Modern Manifestations in North Korea, and Its Implications in Global Relations of the 21st Century*, 2017.
- Souza, Jonas Gregorio De, Denise Pahl Schaan, Mark Robinson, Antonia Damasceno Barbosa, Luiz E. O. C. Aragão, Ben Hur Marimon, Beatriz Schwantes Marimon, et al. "Pre-Columbian Earth-Builders Settled along the Entire Southern Rim of the Amazon." *Nature Communications* 9, no. 1 (2018). <https://doi.org/10.1038/s41467-018-03510-7>.

- Steinmayr, Andreas. "Did the Refugee Crisis Contribute to the Recent Rise of Far-Right Parties in Europe?" *ECONSTOR.EU*. Accessed October 2, 2020. <https://www.econstor.eu/bitstream/10419/181257/1/dice-report-2017-4-50000000000857.pdf>.
- Stengel, Richard. *Information Wars: How We Lost the Global Battle Against Disinformation & What We Can Do About It*. New York: Atlantic Monthly Press, 2019.
- Sterkenburg, Nikki, "Far Right-Right Extremism A Practical Introduction", The RAN Center of Excellence, 2019.
- Stewart, Phil, and Ali, Idrees. "U.S. to withdraw about 12,000 troops from Germany but nearly half to stay in Europe." *Reuters*. July 29, 2020. Accessed August 11, 2020. <https://www.reuters.com/article/us-usa-trump-germany-military/u-s-to-withdraw-about-12000-troops-from-germany-but-nearly-half-to-stay-in-europe-idUSKCN24U20L>.
- Stroud, Natalie Jomini. "Selective Exposure Theories." *Oxford Handbooks Online*, 2014. https://doi.org/10.1093/oxfordhb/9780199793471.013.009_update_001.
- Stytz, Martin R., and Sheila B. Banks. "Toward Attaining Cyber Dominance." *Strategic Studies Quarterly* 8, no. 1 (2014): 55–87. Accessed August 2, 2020. www.jstor.org/stable/26270605.
- Super, Charles M., and Sara Harkness. "The developmental niche: A conceptualization at the interface of child and culture." *International journal of behavioral development* 9, no. 4 (1986): 545–569.
- Suter, Keith. "The Successes and Limitations of International Law and the International Court of Justice." *Medicine, Conflict and Survival* 20, (2004): 344–354.
- Swift, Art. "American's Trust in Mass Media Sinks to New Low." *Gallup* online. September 14, 2016. Accessed August 8, 2020. <https://news.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx>.
- Taylor, Max, Jason Roach, and Ken Pease, eds. *Evolutionary Psychology and Terrorism*. New York: Routledge, 2016.
- Taylor, Emily. 2016. *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality*. GCIG Paper Series No. 23 referring to Morozov 2014. https://www.cigionline.org/sites/default/files/gcig_no24_web_2.pdf
- TC 7-102. (2014, November). Operational Environment and Army Learning. Retrieved August 07, 2020, from https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/tc7_102.pdf
- Tertrais, Bruno. Article 5 of the Washington Treaty: Its Origins, Meaning and Future. NATO Defense College, 2016, www.jstor.org/stable/resrep10238.

- Teslik, Lee Hudson. "Japan and Its Military." Council on Foreign Relations. Council on Foreign Relations, April 13, 2006. <https://www.cfr.org/backgrounder/japan-and-its-military>.
- Thavaselvam, Duraipandian, and Rajagopalan Vijayaraghavan. "Biological Warfare Agents." *J Pharm Bioallied Sci*, Jul-Sep 2010: 179–188. doi: 10.4103/0975-7406.68499.
- The Associated Press. "Iraqis Fleeing ISIS Militants Reveal Fears of Rape, Kidnapping." *NBC News*, June 13, 2014. <https://www.nbcnews.com/storyline/iraq-turmoil/iraqis-fleeing-isis-militants-reveal-fears-rape-kidnapping-n130281>.
- The Deputy Assistant to the Secretary of Defense for Chemical and Biological Defense. *Chemical and Biological Defense Primer*, Department of Defense, October 2001. Accessed August 6, 2020. <https://www.hsdl.org/?view&did=1504>.
- The Economist*. "Emmanuel Macron warns Europe: NATO is becoming brain-dead." 7 November 2019. Accessed August 11, 2020. <https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead>.
- The New York Times. "Syrian Passport by Stadium Stolen or Fake, A.F.P. Reports", November 17, 2015. <https://www.nytimes.com/live/paris-attacks-live-updates/syrian-passport-reportedly-was-stolen-or-fake/>.
- Thompson, A.C. "An Atomwaffen Member Sketched a Map to Take the Neo-Nazis Down. What Path Officials Took Is a Mystery." Pro Publica. Published 20 November 2018; accessed 24 September 2020, <https://www.propublica.org/article/an-atomwaffen-member-sketched-a-map-to-take-the-neo-nazis-down-what-path-officials-took-is-a-mystery>.
- Thornhill, Randy, and Craig T. Palmer. *A Natural History of Rape: Biological Bases of Sexual Coercion*. Cambridge, MA: MIT Press, 2000.
- Thornton, Rod. *Asymmetric Warfare: Threat and Response in the 21st Century*. Polity Press, 2007.
- Tinbergen, Niko. "On Aims and Methods of Ethology." *Zeitschrift für Tierpsychologie* 20, (1963): 410–433.
- Tooze, Adam. *The Deluge: The Great War and the Remaking of Global Order 1916–1931*. London, UK: Penguin, 2015.
- Trakimavicius, Lukas. "Is Russia Violating the Biological Weapons Convention." Atlantic Council, May 2018. <https://www.atlanticcouncil.org/blogs/new-atlanticist/is-russia-violating-the-biological-weapons-convention/>.
- Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia." *The Guardian*. May 16, 2007, accessed August 17, 2020, <https://www.theguardian.com/world/2007/may/17/topstories3.russia>.

- Trivers, Robert L. "Parental Investment and Sexual Selection." In *Sexual Selection and the Descent of Man 1871–1971*, edited by Bernard Campbell, 136–179. Chicago: Adaline, 1972.
- Trump, Donald J. Twitter post. February 19, 2017, 4:57 p.m. Accessed August 13, 2020. <https://twitter.com/realDonaldTrump/status/833435244451753984>.
- Trump, Donald J. Twitter post. January 27, 2019, 8:22 a.m. Accessed August 13, 2020. <https://twitter.com/realDonaldTrump/status/1089513936435716096>.
- U.S. Department of State Bureau of Counterterrorism. "Foreign Terrorism Organizations." Access November 19, 2020. <https://www.state.gov/foreign-terrorist-organizations/>.
- U.S. Department of State. "Human Trafficking." Accessed November 22, 2020. <https://www.state.gov/policy-issues/human-trafficking/>.
- U.S. Congress, House of Representatives, Committee on Homeland Security. *Resolution of Inquiry Regarding Department of Homeland Security Office of Intelligence and Analysis Intelligence Assessment Titled, "Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment."* 111th Cong., 1st sess., 2009, H. Rep. 111–134, 3, congress.gov/congressional-report/111th-congress/house-report/134.
- U.S. Department of Homeland Security. "Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment." Published 7 April 2009.
- U.S. Department of State. "Biological Weapons Convention." Accessed August 13, 2020. <https://www.state.gov/biological-weapons-convention/>.
- U.S. Department of Veterans Affairs. "Chemical and Biological Weapons during Gulf War." Accessed August 12, 2020. <https://www.publichealth.va.gov/exposures/gulfwar/sources/chem-bio-weapons.asp>.
- Umback, Rick. "Huawei and Telefunken: Communications enterprises and rising power strategies." *Strategic Insights*. Australian Strategic Policy Institute, 2019. Accessed August 6, 2020. <http://www.jstor.com/stable/resrep23012>.
- United Nations Office on Drugs and Crime. *Global Report on Trafficking in Persons*. Vienna: United Nations, 2018. https://www.unodc.org/documents/data-and-analysis/glotip/2018/GLOTIP_2018_BOOK_web_small.pdf.
- United Nations Office on Genocide Prevention and the Responsibility to Protect. "Definitions: Genocide, Crimes Against Humanity War Crimes, and Ethnic Cleansing." Accessed November 23, 2020. <https://www.un.org/en/genocideprevention/crimes-against-humanity.shtml>.

- United Nations Women's Rights Unit. "Sexual Violence and Armed Conflict: United Nations Response." *Women2000*, (April 1998). <https://www.un.org/women-watch/daw/public/cover.pdf>.
- United Nations. General Assembly. *Universal declaration of human rights*. Vol. 3381. Department of State, United States of America, 1949.
- United States Air Force Center for Unconventional Weapons Studies. *Chemical and Biological Warfare Overview*. Accessed August 14, 2020. <https://www.airuniversity.af.edu/Portals/10/CSDS/Books/cbwprimer2015.pdf>.
- Ura, Alexa. "Texas officials flag tens of thousands of voters for citizenship checks." *The Texas Tribune*, January 25, 2019. Accessed August 17, 2020. <https://www.texastribune.org/2019/01/25/texas-flags-tens-thousands-voters-citizenship-check/>.
- US Constitution Amendment II. Right to Bear Arms. Passed by Congress September 25, 1789. Ratified December 15, 1791. <https://constitutioncenter.org/interactive-constitution/amendment/amendment-ii>.
- US Office of the Director of National Intelligence. *A Guide to Cyber Attribution*. Washington, DC: ODNI, 2018, Accessed August 14, 2020. https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf.
- Valverde, Miriam. "Trump's travel restrictions survive Supreme Court, fall short of promised Muslim ban." *Politifact*, November 14, 2018. Accessed August 17, 2020. <https://www.politifact.com/truth-o-meter/promises/trumpometer/promise/1401/establish-ban-muslims-entering-us/>.
- Van den Berghe, Annabell. "Humiliation Replaces Fear for the Women Kidnapped by ISIS." *The Guardian*, October, 19, 2014. <https://www.theguardian.com/world/2014/oct/19/isis-forced-marriage-syria-iraq-women-kidnapped>.
- Vandermassen, Griet. "Evolution and Rape: A Feminist Darwinian Perspective." *Sex Roles* 64, (2011): 732–747.
- Vasey, Paul L., Bernard Chapais, and Carole Gauthier. "Mounting interactions between female Japanese macaques: testing the influence of dominance and aggression." *Ethology* 104, no. 5 (1998): 387–398. <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1439-0310.1998.tb00077>.
- Vest, Nathan, and Colin P. Clarke. "Is the Conflict in Libya a Preview of the Future of Warfare?" *Defense One*. Defense One, June 2, 2020. <https://www.defenseone.com/ideas/2020/06/conflict-libya-preview-future-warfare/165807/>.
- Violent Right-Wing Extremism and Terrorism –Transnational Connectivity, Definitions, Incidents, Structures and Countermeasures, Report by Counter-Extremism Project. November 2020. <https://www.counterextremism.com/>

- sites/default/files/CEP%20Study_Violent%20Right-Wing%20Extremism%20and%20Terrorism_Nov%202020.pdf.
- Vygotsky, Lev. "Interaction between learning and development." *Readings on the development of children* 23, no. 3 (1978): 34–41.
- Walker, Shawn, Dan Mercea & Marco Bastos "The disinformation landscape and the lockdown of social platforms." *Information, Communication & Society* 22, no. 11 (August 2019): 1531–1543. Accessed August 8, 2020. doi:10.1080/1369118X.2019.1648536.
- Walton, Calder. "China Will Use Huawei to Spy Because So Would You." *Foreign Policy*, July 14, 2020. Accessed July 15, 2020. <https://foreignpolicy.com/2020/07/14/britain-boris-johnson-china-will-use-huawei-to-spy-because-so-would-you>.
- Walton, Timothy R. *Challenges in Intelligence Analysis: Lessons from 1300 BCE to the Present*. Cambridge, UK: Cambridge University Press, 2010.
- Walton, Timothy. Lecture at James Madison University, March 23, 2020.
- Wang, D., and G. Mark. "Internet Censorship in China: Examining User Awareness and Attitudes." 2015.
- Wang, Peng. "The Crime-Terror Nexus: Transformation, Alliance, Convergence." *Asian Social Science*, vol. 6, no. 6, 18 June 2010, pp. 11–18., doi:10.5539/ass.v6n6p11.
- Wang, Tai-Li. "Does Fake News Matter to Election Outcomes?: The Case Study of Taiwan's 2018 Local Elections." *Asian Journal for Public Opinion Research* 8, no. 2 (May 2020): 67–104. Accessed August 8, 2020. <https://doaj.org/article/108073359c6f4a8e9135b721faeb0155>.
- War." *Journal of Modern Chinese History*, vol. 2, June 2010: 155–172. <https://doi.org/10.1080/17535650701677239>.
- Ward, Antonia. "How Do You Define Terrorism?" *The National Interest*, May 31, 2018. <https://nationalinterest.org/feature/how-do-you-define-terrorism-26058?nopaging=1>.
- Welch, Larry. "Cyberspace – The Fifth Operational Domain." IDA. 2011. Accessed August 17, 2020. <https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx>.
- Whitehouse Archives, "Address to a joint session of the 107th Congress", by President George W. Bush, September 20, 2001, in *Selected Speeches of George W. Bush 2001–2008*: 68. Accessed August 24, 2020, <https://george>

- wbush-whitehouse.archives.gov/infocus/bushrecord/documents/Selected_Speeches_George_W_Bush.pdf.
- Whiten, Andrew, and Richard W. Byrne. "The manipulation of attention in primate tactical deception." (1988). <https://psycnet.apa.org/record/1988-98392-016>.
- Wike, Richard, Bruce Stokes, and Katie Simmons. "Europeans Fear Wave of Refugees Will Mean More Terrorism, Fewer Jobs." *Pew Research Center's Global Attitudes Project*, July 11, 2016. <https://www.pewresearch.org/global/2016/07/11/europeans-fear-wave-of-refugees-will-mean-more-terrorism-fewer-jobs/>.
- Williams, Mollie and Daniel C. Sizemore. "Biologic, Chemical, and Radiation Terrorism Review." *StatPearls [Internet]*, February 2020. Accessed August 16, 2020. <https://www.ncbi.nlm.nih.gov/books/NBK493217/>.
- Wilson, Margo, and Martin Daly. "Competitiveness, Risk Taking, and Violence: The Young Male Syndrome." *Ethology and Sociobiology* 6, 59–73.
- WIRES, NEWS. "Brussels Jewish Museum Shooter 'an Angry French Teen' Who Was Radicalised in Jail." *France 24*, March 8, 2019. <https://www.france24.com/en/20190308-brussels-jewish-museum-attack-mehdi-nemmouche-french-teen-radicalised-jail>.
- Wofford, Taylor. "ISIL, ISIS or IS? The Etymology of the Islamic State." *Newsweek*, September 16, 2014. <https://www.newsweek.com/etymology-islamic-state-270752>.
- Woodward, Calvin and Hope Yen. "AP FACT CHECK: Trump's misleading rhetoric on immigrants." *AP News*, April 29, 2019. Accessed August 13, 2020. <https://apnews.com/fb21a03e4d2246b1926830e8def6e999>.
- Zhang Yiwu (2008) Cultural Challenges of Globalization, *Journal of Contemporary China*, 17:57, 733–746, DOI: 10.1080/10670560802253485.
- Zhang, Xing-Ping, and Xiao-Mei Cheng. "Energy consumption, carbon emissions, and economic growth in China." *Ecological Economics* 68, no. 10 (2009): 2706–2712.
- Zilinskas, Raymond A. "Second-Tier Suppliers of Biological Warfare Technology, Equipment, and Materials: The Potential Roles of China, India, and Cuba." James Martin Center for Nonproliferation Studies, January 2008. Accessed August 14, 2020. <https://www.hsdl.org/?view&did=716634>.
- Zilinskas, Raymond A. "The Soviet Biological Weapons Program and Its Legacy in Today's Russia." National Defense University, July 2016. Accessed August

- 14, 2020. https://inss.ndu.edu/Portals/68/Documents/occasional/cswmd/CSWMD_OccasionalPaper-11.pdf?ver=2016-07-18-144946-743.
- Zuhair, Diab. "Syria's Chemical and Biological Weapons: Assessing Capabilities and Motivations." *The Nonproliferation Review/Fall 1997*. <https://www.nonproliferation.org/wp-content/uploads/npr/diab51.pdf>.

Authors' bios

Zoë BRAMMER will soon be graduating from Clark University with degrees in International Relations and Economics. Her primary area of interest is security studies, and she hopes to produce a longer work on cyber threat and pandemic disease preparedness and response in the coming year. She thanks the program for the opportunity to be published, and Professor Paulina Piasecka especially for her cyber security expertise.

Steven DAVIC is an undergraduate honors student at James Madison University (JMU) pursuing a B.S. in Intelligence Analysis and Biological Anthropology with minors in Biology and Honors Interdisciplinary Studies. Prior to attending JMU he served in the United States Marine Corps for five years, where he deployed twice as an infantry mortarman and spent a year as a research fellow at the Marine Corps Warfighting Laboratory. He plans to continue his education in a Ph.D. program to study cognitive science. Steven can be contacted at davicsteven@gmail.com

Lauren EDSON will be a senior at James Madison University, majoring in Intelligence Analysis and minoring in Political Science. Within the intelligence analysis program, Lauren has been focused on studying China through her analytical assignments. She is simultaneously learning Mandarin Chinese through online tutoring and university classes and hopes to use this skill in her future career. Lauren is also interested in the proliferation of biological and chemical weapons, as exemplified by research completed in the Collegium Civitas summer program, as well the senior capstone project required by her university. Lauren will continue

researching the effects of biotechnology on the proliferation of biological and chemical weapons throughout her senior year which will culminate into a final brief presentation on the topic in front of professors, students and potential employers. Lauren can be contacted via email (laurensessedson@gmail.com) to further discuss this topic or the findings of this paper.

Sarah GOSSETT is a master's candidate at the Patterson School of Diplomacy and International Commerce and a former U.S. Army National Guard Public Affairs Specialist. Her focuses are diplomacy, international security, culture, commerce, and political-military affairs, specializing in Sub Saharan Africa and China. She earned a Bachelor of Science in 2017 in Integrated Strategic Communication from the University of Kentucky, where she focused in public relations, political science and global studies and studied international media and communication abroad in South Africa, China, and the United Kingdom.

Andrew M. HOLUB received his PhD in psychology from Oakland University in Rochester, MI, USA, where he is currently a Special Lecturer. His research focuses on the application of evolutionary theory to understanding human violent and sexual behaviours.

Yasmeen JONES is a graduate student earning her master's degree of Science at Syracuse University School of College of Arts and Science and Maxwell School of Citizenship and Public Administration. She is currently studying Forensic Science and Global Security Studies. For the past six years she has lived and studied in Syracuse, NY – first for her bachelor's degree of Science and now her graduate degree. Following her studies, she seeks to work for and transfer the skills she has developed over the years to the government as an Intelligence Analyst. Her motivation and drive to continue with her studies is in part thanks to her supportive family. She is grateful for her parents and hopes to make them proud of the work she has been doing in and out of school. On a personal note, she loves to read, cook, travel to different places, listen to music, and workout in her free time when she is not focused on studying for exams or writing papers. Later in life, she hopes to gain more experience by traveling worldwide to learn new cultures and experience new foods. By May 2021 she plans to graduate from Syracuse University and start her career for the US government as an Intelligence Analyst.

McKenzie KOTARA is a student at the University of Texas at Austin studying Anthropology and Sociology. She aims to work in the law enforcement field one day and dreams of working for the Federal Bureau of Investigation. She can be reached at: mckenziekotara@utexas.edu

Marianne PERKINS is a student of international affairs and German studying at ETSU in Johnson City, Tennessee. She is passionate about international affairs and development as well as human rights. She assisted as an intern in making Peace Corps Volunteers' grant applications stronger to ensure their projects receive as much funding as possible. Her experience with East Tennessee State University's Alternative Break program led her to be passionate about human rights issues domestically. In studying similar issues internationally through the Peace Corps and international relations courses, she widened her understanding of how these issues affect people across borders. She is further interested in being involved in humanitarian law and understanding these issues' legal workings.

Matthew PIERRO is an undergraduate student studying Peace, War, and Defense and Global Studies at the University of North Carolina at Chapel Hill. Matthew is interested in international security and warfare, as well as international development efforts. His regions of interest include the Middle East, Central Asia, and Eastern Europe. For comments on this paper or any business-related inquiries, Matthew can be reached at the email address mpierro1066@gmail.com

Sami SHIHADAH is a Non-Proliferation, Terrorism, and Financial Crime M.A candidate at Middlebury Institute for international studies. He was born in Syria, and due to the civil war was forced to seek political asylum in Spain from 2012 to 2016. His research interests include international relations and security studies. After experiencing firsthand the devastating consequences of the Syrian war, and witnessing the rise of radicalization and terrorism amongst the Syrian population, he now seeks to become an expert on state and non-state terrorism.

Jefferson T. STAMP is a California lawyer and a current graduate student in a master's degree program focusing on international security, non-proliferation and terrorism studies at the Middlebury Institute of International Studies in Monterey, California. Mr. Stamp may be contacted through the California State Bar website <https://www.calbar.ca.gov> or through his student email address: jstamp@middlebury.edu.

Theodore WARNER is a graduate student at the University of Texas at Austin pursuing a dual master's degree in Global Policy Studies and Russian, East European and Eurasian Studies. He studied abroad in Irkutsk, Russia in 2018 and received his Bachelor of Arts in Political Science from Texas State University in 2019. His research interests include political media and communications, emerging threats in cybersecurity, disinformation, and post-Soviet political culture.

Kathryn WESTON is a student studying at the University of Missouri–Columbia as a Philosophy major and Peace Studies minor. She hopes to study the Russian language in Ukraine following the easing of travel restrictions. After graduation, she intends to pursue a master's degree in Security Studies and enter the security field; she is currently interested in studying the history, philosophy, and strategy of far-right movements across the globe. In her spare time, she likes to read philosophy, Russian literature, and books on security; hike and go to the gym; and experiment with hot chocolate recipes.

Andrée WIETOR holds degrees in philosophy and literature from the University of Tübingen, Germany, and a master's degree in European studies from the College of Europe in Natolin, Warsaw. After graduating in 2011, she joined the civil service in Luxembourg. Her main interests are political theory, foreign policy, international relations, migration, justice, security, and human rights. She currently is enrolled as a law student at the University Paris II Panthéon-Assas. Email: andree.wietor@coleurope.eu; andree.wietor@etudiants.u-paris2.fr

It is our pleasure to present a third scholarly volume bringing together a unique series of research papers by talented students – participants in the Security and Society in the Information Age program held at Collegium Civitas University in Warsaw, Poland. In 2020, due to the pandemic, the program was held for first time online and included a component on the security-related implications of Covid-19.

The students took part in a fully-fledged online course followed by an online research internship at the Terrorism Research Center. This book presents the results of their work – research papers devoted to contemporary security threats. The contributors not only analyzed the issues but also looked for solutions and these papers include recommendations for policy makers.

We hope you will find this book interesting and valuable and we cordially invite you to learn more about the Security and Society in the Information Age program at: www.securityandsociety.org

ISBN 978-83-66386-15-0

