AMERICAN UNIVERSITY
NATIONAL SECURITY LAW BRIEF

American University Washington College of Law
Washington, D.C.

AMERICAN UNIVERSITY

NATIONAL SECURITY LAW BRIEF

lex
cautela

AMERICAN UNIVERSITY
NATIONAL SECURITY LAW BRIEF

THE FORUM ON NATIONAL SECURITY LAW

Volume X • Supplement, Number I • Summer 2019

American University Washington College of Law
Washington, D.C.

AMERICAN UNIVERSITY NATIONAL SECURITY LAW BRIEF

The Forum on National Security Law, Volume X, Number 1 (Summer 2019)

ISBN: 9781081902056

Founded in April 2009, the *American University National Security Law Brief* is the nation's first student-run law school publication to focus on the rapidly evolving field of national security law. The publication is published twice a year, with a complementary online component, and is edited and published by students at American University Washington College of Law.

The views and opinions expressed in the articles are solely those of the respective authors and do not necessarily represent those of the authors' employers, the publication, the editorial board, American University, or Washington College of Law.

The Brief welcomes manuscript submissions on relevant topics in national security law and policy.

For more information about the publication, submissions, or permissions, please visit the brief's website.

Website: nationalsecuritylawbrief.com
Twitter: @AUNatlSecLaw
Facebook: @AUNatlSecLaw
LinkedIn:
linkedin.com/company/AUNatlSecLaw

Bluebook abbreviation: AM. U. NAT'L SEC. L. BRIEF

American University National Security
Law Brief Washington College of Law
American University
4300 Nebraska Avenue NW
Washington, DC 20016

Cover and design by Kevin D. Reyes (consulting editor) (kevindreyes.com)
Printed by Kindle Direct Publishing, an Amazon Company

AMERICAN UNIVERSITY
NATIONAL SECURITY LAW BRIEF

THE FORUM ON NATIONAL SECURITY LAW

Volume X • Supplement, Number I • Summer 2019

Contents

AMERICAN UNIVERSITY

NATIONAL SECURITY LAW BRIEF

EDITORIAL NOTE

Dear Readers,

The National Security Law Brief is excited to publish the second issue of the Forum on National Security Law. This issue, completed with the help and support of the Volume IX editorial board, is a project designed to increase the Brief's scope by providing an opportunity for practitioners and students alike to explore debates in national security law and policy through short, topical pieces.

This issue covers a range of contemporary topics, from the rules of engagement for responding to cyber terror groups to the national security concerns of Chinese State-owned enterprises engaging in Foreign Direct Investment. This issue also considers the status of the U.S. Political Offense Exception to extradition and applies it to the case of U.S.-based cleric Fethullah Gülen, who is sought by Turkish authorities for his alleged involvement in the 2016 coup attempt. Our final article considers cyber risk to the 2020 Census and considers ways to protect our first fully-electronic decennial population survey from the potentially devastating effects of cyber-attacks and covert manipulation.

This issue analyzes the ways that the field of national security law is changing through the advancement of field-leveling technologies, and the ways that U.S. foreign policy must adapt to the pressures of growing geopolitical competition. Our authors are each contributing to salient discussions within the field of national security law that impact U.S. interests. Through the Forum on National Security, we hope to contribute to the constantly shifting debates and developments in National Security scholarship. Thank you for patronage.

Sincerely,

Tucker Kelleher-Brozost
Editor-in-Chief

RESPONDING TO A CYBER 9/11: OBSTACLES TO RECOGNIZING "CYBER ARMED GROUPS" UNDER INTERNATIONAL HUMANITARIAN LAW

By: Anthony Bjelke[*]

INTRODUCTION

Few events in the history of the United States have had as lasting and profound an effect as the terrorist attacks of September 11th, 2001. It not only represented a singular tragedy in our history, but also represented a paradigmatic shift in the way the United States addressed warfighting— contending with an armed group with potential worldwide scope and little if any state involvement. In the same time frame, the development of the internet represented a similar shift. Among the myriad topics related to the development of the internet, "cyberattacks" represent one of the more interesting and challenging from a legal perspective.

Unlike in mainstream regulation of the internet,[1] where developments are mostly based on the evolution of the architecture through new consumer applications[2] connected to the internet and primarily influenced by consumer preferences, the regulation of the internet in the context of cyberattacks and cyberwarfare more predominantly relies on the applicable law and the constraints of system architecture.[3]

Much ink has already been spilled in the service of determining equivalence between nation-state offensive actions in the "real world" as opposed to cyberspace, and because of the nature

---

[*] *Juris Doctor*, American University Washington College of Law, 2020.

[1] Regulation of commercial and general civilian uses of the internet.

[2] *E.g.*, Social Media, Consumer Internet of Things Devices, etc.

[3] *See* Lawrence Lessig, *The Laws of Cyberspace*, Taiwan Net '98 (Mar. 1998) (discussing the four major categories of regulation of behavior in cyberspace: laws, norms, architecture, and markets).

of international law, and more specifically international humanitarian law (IHL) and the laws of armed conflict (LOAC), these examinations are essential.[4]

A major talking point for those in the business of protecting American assets from cyber-related damage is that they are trying to avoid a "Cyber Pearl Harbor."[5] This is an important consideration to be sure, but perhaps a better way of framing the discussion—and a more productive one—is trying to improve at combatting an even more terrifying threat, a "Cyber al-Qaeda."

As with much in the cyber context, it may be difficult to develop a meaningful understanding of what such an entity could look like, and what sort of efforts it would undertake. It would be especially difficult to think of it in a context where there is no support from a nation-state, either explicit or tacit, as was the case with al-Qaeda's operations in Afghanistan. While this paper will continue to call this theorized group "Cyber al-Qaeda"[6] it may be easier to set this discussion in the context of a closer hypothetical, asking the following question: how the international community would have responded under the law of armed conflict if the hacker group Anonymous had actively gone to war with the government of Bashar Al-Assad in Syria? Throughout the early days of the Syrian Revolution, Anonymous was trolling government websites and infrastructure, under the justification of standing up to tyranny.[7]

---

[4] *See infra* Section I.A.

[5] James Stavridis, *The United States Is Not Ready for a Cyber-Pearl Harbor*, FOREIGN POLICY (May 15, 2017), https://foreignpolicy.com/2017/05/15/the united-states-is-not-ready-for-cyber-pearl-harbor-ransomware-hackers-wannacry/.

[6] It is important to note, however, that this paper does not presume a specific objective, ideology, or set of tactics to the theorized groups.

[7] Jeb Boone, *Syrian Electronic Army Revealed: Anonymous Hacks SEA Website, Dumps Data*, GLOBAL POST (Sept. 3, 2013), https://www.pri.org/ stories/2013-09-03/syrian-electronic-army-revealedanonymous-hacks-sea-website-dumps-data; Andy Greenberg, *Anonymous Hackers Swat At Syrian Government Websites in Reprisal for Internet Blackout*, FORBES (Nov. 30, 2012), https://www.forbes.com/sites/andygreenberg/2012/11/30/anonymous-hackers-swat-at-syrian-government-websites-in-reprisal-for-internet-blackout/ #5f4c5384707a; Sarah Kessler, *Anonymous Hackers Take Down Syrian Ministry*

What would have happened, however, if they more actively engaged in offensive and aggressive cyber operations? Anonymous has no allegiance to a country and as far as we know is not supported by a traditional nation-state, and its members span the globe.[8] Were it to engage in hostilities against a nation-state, there is little doubt practically that the target nation and/or its allies would respond, but under international law, there is still an open question as to how such an entity would be characterized?[9]

This paper will seek to outline how international law should consider attacks by "cyber armed groups" within the context of IHL and LOAC and explain why the current precedent for non-international armed conflicts (NIACs)[10] is incomplete for protecting against groups that may not manifest as a traditional armed group, but nevertheless can use the internet to cause physical or economic harm that normally only an armed group or a state could accomplish.

First, the paper will address necessary threshold questions, including (1) can a cyber intrusion rise to the level where it should be considered an "attack" for IHL and LOAC purposes, and (2) if so, can the perpetrators of such an attack be considered an armed group by way of analogy to traditional NIAC related precedent. Second, this paper will examine issues that are uniquely acute in the cyber realm, such as difficulties associated with attribution and

---

of Defense Website, MASHABLE (Aug. 8, 2011), https://mashable.com/2011/08/08/anonymous-syria/#DqkLWAnjVEqo.

[8] *See* Brian B. Kelly, *Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform*, 92 B.U. L. Rev. 1663, 1676-83 (2012) (providing a description of hacktivism in general and Anonymous in particular).

[9] This latter point is especially apt when discussing potential kinetic responses, as has been frequently discussed as a possible response to cyber-attacks by some within the legal community. *See, e.g.*, Stewart Baker, *Thinking the Unthinkable About Responding to Cyberattacks*, STEPTOE CYBERBLOG (Aug. 23, 2018), https://www.steptoecyberblog.com/2018/08/23/thinking-the-unthinkable-about-responding-to-cyberattacks/; Phil Osborn, *Air Marshal Phil Osborn on Intelligence and Information Advantage in a Contested World*, ROYAL U.S. INST. (May 18, 2018), https://rusi.org/event/air-marshal-phil-osborn-intelligence-and-information-advantage-contested-world.

[10] Conflicts in which at least one belligerent is not a state actor.

assessments of proportionality and discerning the line between criminal and military responses. Finally, this paper will propose additions to the present factors[11] considered when assessing whether an "armed group" exists, focusing primarily on measuring the effects of a group's actions rather than its organizational characteristics.

I. THRESHOLD QUESTIONS

The idea of a "Cyber al-Qaeda" from a legal perspective presumes fairly substantial characteristics of the group and of international law, and it is important to hammer out several points before proceeding to further discussions of how to respond to such a Cyber al-Qaeda. First, for the purposes of definitional simplicity, this paper assumes all or almost all of the actions of this hypothetical organization are in cyberspace. This purposely excludes hybrid organizations—to wit, a group such as ISIS perpetrating cyber-attacks to complement their traditional attacks or using cyber intrusions to improve the effectiveness of physical attacks.[12]

Before those technical considerations, it is worth discussing briefly why it would be a positive and useful step to be able to classify a Cyber al-Qaeda type organization as a cyber armed group under the traditional rules for Non-International Armed Conflicts. In the context of traditional warfare, the designation provides flexibility to the rules of war that allow for practical and effective defense where non-governmental groups rise to a level of organization and lethality that exceeds the ability of a state's law enforcement apparatus to respond effectively.[13] There are, of course, fundamental questions of whether as a broader matter, cyber

[11] As specified in *Prosecutor v. Haradinaj*, Judgement IT-04-84-T (Apr. 3, 2008).

[12] Ahmed Salah Hashim, *State and Non-State Hybrid Warfare*, OXFORD RES. GRP. (Mar. 30, 2017), https://www.oxfordresearchgroup.org.uk/blog/state-and-non-state-hybrid-warfare.

[13] Geneva Convention Relative to the Treatment of Prisoners of War art. 3, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

warfare tactics are fundamentally distinct from traditional warfare to such an extent that it would be impossible or impractical to assume that the same rules applied across the board.

From a historical perspective, it is hard to draw a functional distinction between cyber war tactics and traditional warfare. Looking at the issue from an effects-based perspective, cyber-attacks are generally designed to be destructive and disruptive to the target nation/group in some way. From that perspective, it may be more logical to contend that while the methods of attack have certainly changed in a massive and undeniable way, the evolution from the age of steel to the age of silicon may be no more fundamental a change than the evolution from the bronze age to the iron age.

What cyberwarfare represents is therefore a simple evolution in the weapons of war, not the war itself. While arguments could and have been made that there is a fundamental distinction between the battlefields on which cyber wars are fought, cyber-attacks that rise to the level of cyber warfare will almost certainly have physical impacts, whether it be the overloading of a server causing damage or a fire, an attack on a dam's control systems causing flooding and destruction, or an intrusion into the systems of a gas plant causing explosions. Additionally, as with the Russian invasion of Crimea in 2014, these tactics are often employed as complements to "traditional" warfare.[14]

By recognizing (1) that there is not a sufficiently meaningful distinction between "traditional" warfare and cyber warfare to justify an entirely distinct set of laws of cyber armed conflict, and (2) that there may be, nonetheless, situations where cyber bad actors are entirely web-based, it is important to make sure that the U.S. and broader international community has both clarity as to how the community should think about these theoretical bad actors when

[14] AMOS C. FOX & ANDREW J. ROSSOW, INSTITUTE OF LAND WARFARE, NO. 112, MAKING SENSE OF RUSSIAN HYBRID WARFARE: A BRIEF ASSESSMENT OF THE RUSSO-UKRAINIAN WAR 2 (Mar. 2017), https://www.ausa.org/sites/default/files/publications/LWP-112-Making-Sense-of-Russian-Hybrid-Warfare-A-Brief-Assessment-of-the-Russo-Ukrainian-War.pdf.

presented with them, and an understanding of what steps can be taken to respond within the LOAC and IHL context.

A. Can a cyber intrusion be an "attack?"

As a general matter, a malicious cyber operation can be considered an armed attack that can be responded to by force, as publications such as the Tallinn Manual and Tallinn Manual 2.0 contend and—in the context of non-state groups—lead Tallinn Manual author Michael Schmitt allows in subsequent writings.[15] The Tallinn Manual itself defines a "cyber-attack" as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[16]

This definition is apt, as it is both closely analogous to the traditional definition of an armed attack, and it remains easy to imagine situations in which the definition could be met, such as where a cyber operation was intended to cause a critical malfunction at a nuclear power plant, a large dam near a city, or a residential power grid during a blizzard. It is also easy to imagine these same systems being attacked by means of physical sabotage, which could be raised to the level of an armed attack under traditional law of war principles.

A focus on the effects of an action are especially important in the cyber context where so much of the work prior to the deployment of a cyber "weapon" is undetectable and may not look like traditional preparation for an attack. Conversely, so much of the damage that can be caused by these sorts of actions occurs after an enter key is pressed and the malicious actor walks away from their computer, partially if not mostly out of the hands of the individual or group who initiated the action. Whereas traditional analysis of attacks—and then the rights of other nations to

---

[15] Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum, Peacetime Cyber Responses and Cyber Operations*, 8 Harv. Nat'l Sec. J. 239 (2017).
[16] *Id.*

respond—is based on a left of boom/right of boom scale, where to the left of boom there is a point at which the attack becomes "imminent,"[17] in the case of cyber-attacks, that scale may not be quite as helpful.

B. Can the perpetrators of a cyber-attack be an "armed group" under the Tallinn Manual?

Once it is established that a cyber intrusion can rise to the level of an "attack" for international law purposes, it is then essential to ask whether a group connected through and carrying out harmful acts purely over the internet—a Cyber al-Qaeda for the purpose of identification—could be considered an "armed group" for purposes of international law. This is a tricky question to analyze, and given the existing precedent, the answer could easily be no. Discussed in writings by Michael Schmitt on how one should think about threat response in the framework of the Tallinn Manual is the contention that the use of force could be justified against a non-state group.[18] That assertion is conditioned, however, on the non-state group being within the territory of a state that is either unable or unwilling to stop the actions.[19]

Schmitt notes some disagreement over whether the right to state self-defense extends to the cyber context, noting that while the United States and NATO allies have adopted that view, others cite the opinion of the ICJ in a Palestinian territory case and in *Congo v. Uganda* for the proposition that the opposite is the case.[20] An

---

[17] A traditional metaphor for imminence using in instructing on this topic being an army on the other side of a hill moving towards a border. *See, e.g.*, Ashley Deeks, *"Imminence" in the Legal Advisor's Speech*, LAWFARE (Apr. 6, 2016, 7:00 AM), https://www.lawfareblog.com/imminence-legal-advisers-speech (examining the position of State Department Legal Advisor Brian Egan with regards to *jus at bellum* principles of imminence and self-defense).

[18] *See* Schmitt, *supra* note 15.

[19] *Id*. at appx. 1.

[20] *Id*. (citing *Legal Consequences of the Construction of a Wall In the Occupied Palestinian Territory*, Advisory Opinion, 2004 I.C.J. 136 (Jul. 9, 2004) and *Armed Activities in the Congo (Dem. Rep. Congo v. Uganda*.) 2005 I.C.J. 168

important question with regard to that last assertion is whether or not it then matters that a non-state group is specifically labeled an "armed group" if it would be legitimate to use force against the group anyway.

The Tallinn Manual 2.0 ("the Manual") addresses the issue of non-state actors under the category of areas not *per se* regulated by international law.[21] The Manual contends that cyber operations by non-state actors do not amount to the use of force on the basis that only states may undertake such acts.[22] The Manual does, however, contemplate that non-state actors can be said to be subject to the law of armed conflict where they engage in cyber operations "related to an armed conflict."[23] This carves out an exception to the above stated contention, but only to apply it to instances where the non-state actor is engaged in an armed conflict, which would itself require a finding that the non-state actor was an "armed group" for purposes of non-international armed conflicts.[24] Rule 83 of the Manual states:

> A non-international armed conflict exists whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring

(Dec. 19, 2005), as well as SC Res. 1369, UN Doc. S/RES/1368 (Sept. 12, 2001)).

[21] NATO Coop. Cyber Def. Ctr. Of Excellence, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, 168,174-76 (Michael N. Schmitt ed., 2d ed. 2017) [Hereinafter Manual 2.0].

[22] *Id.* at 175 (outlining the breaches which cannot be attributed to non-state actors—including breaches of sovereignty, constituting intervention, and allowing the use of force—and noting that this determination is made "irrespective of any consequences caused by such operations," and only contemplating a contrary view with regards to breaches of sovereignty).

[23] *Id.* at 175-76 (outlining limited situations where non-state actors can be brought into the ambit of international law regulation for cyber operations).

[24] *Id.* at 385 (contending that the Manual's rules with regards to characterization as non-international armed conflict essentially acts as a general restatement of Common Article 3 of the Geneva Conventions of 1949 with regards to the duration, intensity, and organization required for the existence of a non-international armed conflict).

> between governmental armed forces and organized armed groups, or between such groups. The confrontation must reach a minimum level of intensity and the parties involved in the conflict must have a minimum degree of organization.[25]

The Manual does provide for the possibility that cyber actions alone could result in the existence of a non-international armed conflict in "exceptional cases," but notes that findings to that effect are made difficult as a result of the level of organization and intensity of hostilities required.[26] The Manual also provides a carveout that non-state actors could violate international humanitarian law or the law of armed conflict through cyber operations, but that the effect of that would be the application of international criminal law to the individuals. The only time the rules contemplate that a state could respond by use of countermeasures against the acts of a non-state actor in the cyber context is under a plea of necessity, or under a self-defense theory.[27] Stated broadly, states under the Manual would be able to take defensive actions if attacked, but only to a certain limit.

While this position allows for a fair amount of latitude for states in responding to attacks by non-state actors, it also underestimates the potency of cyber conflict by focusing on the process of the attacks rather than the practical impacts that a purely cyber-attack could have on a state. As has been promoted in the cyber context in a number of instances where legal scholars are attempting to attune traditional law to cyberspace, a better method for analysis would be an effects-based test, which would undoubtedly result in a finding that in the cyber arena non-state actors are even more powerful than their traditional law counterparts, as—generally speaking—the power differential

[25] *Id.*
[26] *Id.*
[27] *Id.* at 175.

between states and non-state actors is significantly less stark than in traditional warfare situations.[28]

It is also important to be able to designate such non-state groups as armed groups for another key reason, territoriality. Action under the Schmitt/Tallinn theory, as discussed above, conditions the use of force against these non-state actors as requiring either the reluctance or inability of the host nation to stop the attack.[29] This assumes (1) that the attackers are present within one country or a small and controllable cadre of countries, and (2) that the ability to use force against that group would be limited within the territory of those states that would be unable or unwilling to stop the attack. Since 9/11 and the beginning of the global war on terrorism, the United States and allies have asserted that they are engaged in a "global NIAC" against al-Qaeda and affiliated forces in an effort to assure that they can effectively fight back against potential attacks.[30] This capability is, if anything, more essential in the cyber context where the whole idea of territorial boundaries is fuzzy, and attribution can be difficult.

---

[28] *See, e.g.*, Forrest B. Hare, *Precisions Cyber Weapon Systems: An Important Component of a Responsible National Security Strategy?*, 40 CONTEMP. SEC. POL'Y 193 (2019); Paul K. Davis, *Effects-Based Operations: A Grand Challenge for the Analytical Community*, RAND CORP., 8 (2001), https://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR1477.pdf.

[29] *See* Schmitt, *supra* note 15, at appx. 1.

[30] *See* Andreas Paulus & Mindia Vashakmadze, *Asymmetric War and the Notion of Armed Conflict-A Tentative Conceptualization*, 91 Int'l Rev. Red Cross 95 (2009) (contending that the decision by the U.S. Supreme Court in *Hamdan v. Rumsfeld* stands for the proposition that there is a global NIAC as a matter of U.S. law). *Cf.* Manual 2.0, *supra* note 21, at 386 (discussing the debate amongst scholars of international law on whether the term "in the territory of *one* of the [parties]" in Common Article 3 of the Geneva Conventions necessarily restricts the reach of a NIAC to a single state or functionally means in the territory of any of the parties (emphasis added)). *But see* Johnathan Horowitz, *Reaffirming the Role of Human Rights in a Time of "Global" Armed Conflict*, 30 Emory Int'l L. Rev. 2041 (2015) (contending that there is not a legitimate justification for the recognition of a "global NIAC" based only on the premise that members of an armed group could cross borders).

C. *Can the perpetrators of a cyber-attack be an "armed group" under the ICTY test in* Haradinaj*?*

It is worth noting that while it is cited authoritatively often across the cyber law field, the Tallinn Manual is not technically binding on anyone. Even if it were to more explicitly contend that a cyber entity can be an armed group, there is potentially controlling precedent from the International Criminal Tribunal for the former Yugoslavia (ICTY), which has a much more stringent definition of what an armed group can be. The Tribunal identified the following factors to be considered when assessing the existence of an armed group:

> Such indicative factors include the existence of a command structure and disciplinary rules and mechanisms within the group; the existence of a headquarters; the fact that the group controls a certain territory; the ability of the group to gain access to weapons, other military equipment, recruits and military training; that ability to plan, coordinate and carry out military operations, including troop movements and logistics; its ability to define a unified military strategy and used military tactics; and its ability to speak with one voice and negotiate and conclude agreements such as cease-fire or peace accords. [31]

Given these factors, it is unlikely that a cyber armed group in the mold of the hypothetical above would be considered an armed group under this precedent. The group could potentially meet the command structure and tactics prongs, and depending on those structures, may be able to reach the negotiation and agreement prong, but depending on how important the physical elements are,

[31] *Prosecutor v. Haradinaj*, Judgement IT-04-84-T at ¶ 60 (Apr. 3, 2008).

such as the existence of a headquarters, movements of troops and logistics, and unified military tactics prongs, a Cyber al-Qaeda may not pass muster. Another potential problem is considering how terms, such as "unified military strategy," "military tactics," "military training," "military equipment," and "military operations," are defined in these contexts.

There has been little need to consider these questions before because the military has clear definitions in combat settings However, this dearth of definition has left few satisfactory answers in public international law. While it is positive that there has not been a full-blown cyber war the impulse to set the rules of the road for cyber issues is pressing. Certainly, there have been attempts, such as the Tallinn Manual or the "agreement" on cyber action between President Obama and Chinese President Xi.[32] These agreements being executed by a pair or a relatively small group of countries, however, gives these sorts of "rules of the road" limited applicability beyond the borders of jurisdictions that have "bought in."

II. ADDITIONAL CONCERNS IN RESPONDING TO AN ATTACK BY A "CYBER AL-QAEDA"

All other considerations on the legitimacy of the use of military force aside, there are a number of other hurdles to clear before an actual instance of the use of force against a cyber adversary could be effectuated. Outlined quickly below are several of those concerns, mostly drawn from or related to the customary

[32] *See* Jack Goldsmith, *What Explains the U.S.-China Cyber "Agreement"?*, LAWFARE (Sept. 26, 2015), https://www.lawfareblog.com/what-explains-us-china-cyber-agreement. *But see* Chris Bing, *Trump Administrations Says China Broke Obama-Xi Hacking Agreement*, CYBERSCOOP (Mar. 22, 2018), https://www.cyberscoop.com/trump-china-hacking-obama-xi-agreement/.

international law considerations of distinction, proportionality, military necessity, limitation, and good faith humane treatment.[33]

A. Targeting

One of the thorniest considerations for *jus in bellum* scholars in the era of pervasive non-state actors involved in warfare—and the fact that warfare is now more often waged in areas with a high concentration of civilians—is the question of who is a legitimate target of offensive force?[34] Without organized armies with insignia and uniforms, a question arises of where the line is drawn between someone merely ancillary or tangentially related to an armed group, and one intimately related to the group enough to be the subject of an attack. This question gave rise to the continuous combatant doctrine, which provides that an individual is protected against being the target of an attack "unless and for such time as they take a direct part in hostilities."[35]

The "continuous combatant function" doctrine—which provides that one cannot be considered a combatant and therefore a lawful target of force—has been litigated thoroughly in the post 9/11 era, where there have been a number of different fact patterns examining the edges of this doctrine.[36] The issues around the edges

---

[33] *The Law of Armed Conflict: Non-international Armed Conflict*, INT'L COMM. RED CROSS (June 2002), https://www.icrc.org/en/doc/assets/files/other/law10_final.pdf.

[34] *Practice Relating to Rule 3. Definition of Combatants, IHL Database*, INT'L COMM. RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule3 (last visited July 31, 2019).

[35] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), Part IV, June 8, 1977, 1125 U.N.T.S. 609. *See also Interpretive Guidance on the Notion of Direct Participation in Hostilities*, INT'L COMM. RED CROSS (2009), https://casebook.icrc.org/case-study/icrc-interpretive-guidance-notion-direct-participation-hostilities.

[36] *See, e.g.*, Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 Int'l L. Pol'y 641 (2010); Shane Reeves, *Bin Laden and Awlaki: Lawful Targets*, Harv. Int'l L. Rev. (2011).

of this doctrine—which roughly fall into two categories, those where the combatant is tangentially related to direct combat or where combat activities are intermittent—could be even more troublesome in cyberspace, where there need not be a direct temporal connection between a combatant being active and damage being done. Of course, there are historical equivalents to that scenario, such as placing mines or time delay devices, but the unpredictable nature of cyber weapons once engaged may make that analogy somewhat thin. Either way, further discussion does need to be had on this topic, and it is probable that most of the decisions on this topic will be operational ones based on specific fact patterns best adjudicated when those facts present themselves and not in the abstract.

B. Proportionality

A very tricky question, even if one assumes that there is a legitimate justification for the use of force, is determining in what form that force will be manifested. Even without the additional wrinkle of cyberspace, questions of what is proportional is a question that is often debated.[37] Determining whether the destruction of an airfield is proportional or appropriate to the downing of a U.S. military personal transport was even a favorite topic of Director Aaron Sorkin, who put forth the same scenario both in his *The American President* and later in *The West Wing* as a means

[37] *See generally* Robert D. Sloane, *Puzzles of Proportion and the "Reasonable Military Commander": Reflections on the Law, Ethics, and Geopolitics of Proportionality*, 6 Harv. Nat'l Sec. J. 299 (2015) (addressing different measurements for determining what is proportional, including a discussion of asymmetric warfare); Alon Margalit, *Did LOAC Take the Lead? Reassessing Israel's Targeted Killing of Salah Shehadeh and the Subsequent Calls for Criminal Accountability*, 17 J. Conflict & Sec. L. 147 (2012) (discussing the report of the Israeli Inquiry Committee on the targeted killing of the commander of a unit of Hamas).

of thinking about the constraints of proportionality in the context of U.S. hegemony in the wake of the end of the Cold War.[38]

The question of proportionality is even trickier in terms of cyberspace, when the question is not whether a kinetic attack on a high value target is equivalent to another but is instead whether physical force is ever a proportional response to a cyber-attack. That question is one far too complicated for a paper addressing this wider topic but suffice it to say that this author would content that a prudent approach in this as in most parts of this topic, would be to examine the effects of the cyber intrusion.[39]

Discussion on this topic has been significant in the wake of an incident in May 2019 where, during a period of heightened hostility and active engagement between Israel and Hamas, elements within Hamas launched a failed cyber-attack on Israeli critical infrastructure, and Israel responded with a rocket strike on the building where the cyber-attack was initiated.[40] Some initially pointed to this incident as a potentially significant step in the development of doctrine in this area.[41] The author, however, would concur with the assessment of Professor Robert Chesney that, given that this attack took place in the context of broad and ongoing kinetic operations, this is not really an incident that provides scholars in this area a great case study for assessing the legal implications of cyber-attacks.[42] Nevertheless, as at least one major power has indicated

---

[38] *The West Wing: A Proportional Response* (NBC television broadcast Oct. 6, 1999); THE AMERICAN PRESIDENT (Warner Bros. 1995).

[39] For more examination of this topic, *see, e.g.*, *The Hackback Debate*, STEPTOE CYBERBLOG (Nov. 2, 2012) (where Stewart Baker, Professor Orin Kerr, and Eugene Volokh debated the merits of allowing for hackbacks); *Cyber Security: Responding to the Threat of Cyber Crime and Terrorism: Hearing Before Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 112th Cong. (2011) (testimony of Stewart Baker).

[40] Robert Chesney, *Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility*, LAWFARE (May 6, 2019), https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility.

[41] *Id.*

[42] *Id.*

they are willing to use kinetic force against cyber adversaries, the incident does provide a starting point for a broader examination of the doctrine.

III. NEW FACTORS TO IDENTIFY "CYBER ARMED GROUPS"

This paper asserts (1) that a cyber intrusion can rise to the level of an "attack" for international law purposes, (2) that a group purely connected by means of the internet may not fall under the category of an "armed group" under the ICTY, (3) that the Tallinn Manual significantly limits the ability of a "cyber armed group" to be identified, and (4) that there are surely situations in which a state would be able to respond such a "cyberattack" were it to have come from a state. Given these limits to the current international framework, it seems essential to try and resolve these tensions.

Given the Tallinn Manual's affiliation with NATO, and its usefulness for cyber operations, applying new principles to broader international law would be preferable. Likely the best way to handle this tension, therefore, is to supplement the current factors put forth by the ICTY for determining whether an organization constitutes an "armed group" for the purpose of non-international armed conflicts.

While there are surely a number of additional factors that could be added, this paper suggests two. By the nature of their construction, and in order to avoid the factors being used to broaden the scope of coverage over traditional groups, these factors would apply exclusively to groups like the hypothetical "Cyber al-Qaeda" whose actions are primarily, if not exclusively, online.

A. Factor One: "where the physical or economic effects of the actions of a group are of a duration and/or intensity where analogous effects in traditional warfare could only be carried out by an armed group or state."

The purpose of introducing this factor into the list of those generally considered by courts and the ICRC when assessing the "armed group" status of an organization is to expand the scope of

the traditional examination of "duration and intensity," one of the key elements looked at when considering armed group status in non-international armed conflicts.[43] In setting forth duration and intensity requirements, the international community sought to draw a line between those ordinary acts of violence which domestic criminal laws were designed to punish, and systemic and coordinated acts of violence above the level that civilian law enforcement is designed to handle.[44]

Drawing this line is important because there are any number of domestic tools for fighting off malicious cyber actors through traditional legal pathways[45] that would normally be more appropriate than the coordinated use of military force. It is important, however, to recognize that while most cyber-intrusions (regardless of whether they are classified as cyber-attacks) would not rise to the level of requiring a military response, there is a line where the use of cyberwarfare by a group could become persistent enough to warrant sustained responses utilizing force. Given the ever evolving and high paced nature of the cyber threat environment, it is essential that this topic be considered prior to it being practically applicable. In the increasingly polarized nature of the world diplomatic order, once an event has happened, ideological and self-interest-based entrenchment determining "rules of the road" would be difficult to say the least.

A major open question that this factor would create, and one that should be discussed further, is how to factor in the effects of an ongoing, self-propagating cyber intrusion. Examples of this sort of tactic can be seen most readily in early examples of hacks such as

---

[43] *Haradinaj*, *supra* note 31, at ¶ 49. *See* Manual 2.0, *supra* note 21, at 385 (identifying the elements of intensity and organization in determining whether there is a non-international armed conflict in the cyber context).

[44] *Id.*

[45] *See, e.g.*, The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* (1984) (providing for criminal penalties for unauthorized uses of computer networks).

the Morris Worm,[46] or more recently in the so-called Stuxnet attacks.[47]

In both those cases, the effects of the cyber bad act went far beyond the point at which the originator "hit send" for lack of a better term, and in both scenarios, there were questions as to whether it was even the intent of the originator to cause damage over such a wide scale and over a prolonged period of time. In the case of the Stuxnet attacks, the conventional story in the public domain was that the virus was designed to specifically target the computers at an Iranian nuclear facility to cause the centrifuges there to malfunction, but, because someone on the network in the facility was connected to the internet, the bug propagated out of control and across the world.[48]

In assessing a Stuxnet style attack, should there be some form of assessment of proximate cause in determining proportionality? If the intent of a Cyber al-Qaeda was to use an exploit to cause a malfunction shutting down the electrical grid in parts of upstate New York, but the exploit gets into the broader system and ends up causing a meltdown at the Indian Point Nuclear Plant, does that potentially unintended downstream effect factor into proportionality? Does assessing the intended versus unintended just create more headaches in the complex world of attribution? Is it even possible to assess intent during the window within which retaliation, cyber or kinetic, would be effective?

---

[46] *The Morris Worm: 30 Years Since First Major Attack on the Internet*, FBI (Nov. 2, 2018), https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.
[47] Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
[48] *Id.*

B. Factor Two: "where the persistent nature of the communications and coordination of members of a group are of such a magnitude as to be akin to those of a traditional armed group or state."

Many of the traditional factors in determining whether an armed group exist are related to physical actions or acquisitions by armed groups as means of demonstrating that there has been coordination and a stable presence by the armed group.[49] This new factor would take into account the incorporeal nature of cyber groups, as they no longer really need a headquarters or territory in order to organize sufficiently to cause harm at a level above that of a criminal organization.

This factor would continue the shift to an effects-based model of addressing cyber bad actors, given the decreased correlation between factors such as effort and manpower, and the practical effects of a given attack. This factor potentially solves some of the issues identified in the discussion of factor one above, tying the effects-based findings above to a similar and connected finding of some sophisticated yet physically decentralized form of organization.

CONCLUSION

This piece may seem somewhat out of time, as much of the literature and study surrounding cyberwarfare is focused on malicious actors attached to governments of nations like China, Russia, and Iran. It may seem somewhat difficult to picture what a "Cyber al-Qaeda" would look like, mostly because we have not seen one in action to date. Although attribution is a significant issue in this field, so far, governments have been able to link most significant cyber incidents to a state actor in one form or another.[50] Present

---

[49] *See Haradinaj, supra* note 31 (discussing factors such as a group having a headquarters, territory, or purchasing military weapons).

[50] *See, e.g.*, *Cyberwarfare by China*, WIKIPEDIA, https://en.wikipedia.org/wiki/Cyberwarfare_by_China (last visited Dec. 5, 2018).

practice, however, does not necessarily indicate future results, and it is entirely possible that some form of decentralized non-state actor with malicious intentions on the internet could emerge. Defining the rules of engagement before that time will aid the international community in responding to these types of attacks.

CHINESE STATE-OWNED ENTERPRISE INVESTMENT: AN ECONOMIC STATECRAFT

By: Bashar H. Malkawi[*]

China has overtaken Japan as the world's second-biggest economy.[1] In a remarkably short span– less than fifteen years– the United States economy has experienced a relatively huge decline vis-à-vis China on a nominal GDP basis.[2]

China's remarkable economic growth, fueled by an opening of markets, globalization, and booming free trade, has provided immense financial benefit to Chinese companies.[3] The free market open rules trading system has "led to the establishment of China as a major global exporter."[4] As China's economy has boomed, China has looked increasingly abroad for investment opportunities to both employ its financial resources and provide long-term growth for its citizens.[5]

Many of China's large companies are state-owned enterprises (SOEs), and SOEs are the primary drivers of Chinese investment.[6] Chinese SOEs receive preferential treatment in terms of access to capital and licensing, winning government procurement

---

[*] Bashar H. Malkawi is Dean and Professor of Law at the University of Sharjah, United Arab Emirates. He holds S.J.D in International Trade Law from American University, Washington College of Law and LL.M in International Trade Law from the University of Arizona.

[1] *See Projected GDP Ranking* (2018), STATISTICS TIMES (Apr. 2, 2018), http://statisticstimes.com/economy/projected-world-gdp-ranking.php.

[2] *See* WAYNE M. MORRISON, CONGRESSIONAL RESEARCH SERVICE, CHINA'S ECONOMIC RISE: HISTORY, TRENDS, CHALLENGES, AND IMPLICATIONS FOR THE UNITED STATES, 8 (2018).

[3] *Id.*

[4] *See* Zhong Nan & Jing Shuiyu, *Steps Will Spur Imports as Export Growth Slows*, TELEGRAPH (Jan. 22, 2019), https://www.telegraph.co.uk/china-watch/business/china-import-and-export/.

[5] *Id.*

[6] *See* CHINA INSTITUTE, UNIVERSITY OF ALBERTA, STATE-OWNED ENTERPRISES IN THE CHINESE ECONOMY TODAY: ROLE, REFORM, AND EVOLUTION, 2-4 (2018).

contracts, and obtaining regulatory approval within China.[7] They are deployed to advance Chinese governmental aims and "serv[e] political goals, including fostering indigenous innovation, supporting social stability and crisis response in China, and advancing economic initiatives abroad, such as 'One Belt, One Road.'"[8]

By definition, all SOEs raise concerns because of their connection to their home states. These anxieties over state-owned businesses are not unique to Chinese companies, and all SOEs in other countries provoke the same concerns.[9] Investments made by states trigger different regulatory sensitivities compared to considerations raised by private companies because of the possibility that in conducting business, government-owned or -controlled entities may utilize political motivations and substitute political ambitions instead of or in addition to profit-making.

These concerns are tied to any government-owned business that potentially subjugates private market interests to the political interests of the state or, alternatively, acts with additional motives than traditional market incentives.[10] Indeed, such concerns are not entirely new. An example of prior concerns related to government-owned businesses and their investment decisions was the opposition over Dubai Ports World's attempt to invest in the U.S.[11] In 2007, Dubai Ports World—an institution owned by the government of the

---

[7] *See* Wendy Leutert, *China's Reform of State-Owned Enterprises*, 21 ASIA POL'Y 83, 86 (2016).

[8] *Id.*

[9] *See* Ines Willemyns, *Disciplines on State-Owned Enterprises in International Economic Law: Are We Moving in the Right Direction?*, 19 J. Int'l Econ. L. 657, 661 (2016).

[10] *See Sovereign Wealth Fund Acquisitions and Other Foreign Government Investments in the United States: Assessing the Economic and National Security Implications*: *Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 110th Cong. 4 (2007) (testimony of Edwin M. Truman, Senior Fellow, Peterson Institute for International Economics).

[11] *See* Bashar H. Malkawi, *The Dubai Ports World Deal and U.S. Trade and Investment Policy in an Era of National Security*, 7 J. World Inv. & Trade 443, 452 (2006).

Emirate of Dubai—sought to acquire port terminals located in the U.S.[12] Members of the U.S. Congress, concerned about a foreign government controlling the flow of goods and people into the U.S., voiced strenuous opposition to the move on national security grounds. In this respect, Chinese SOEs are no different than other state-owned businesses.[13]

However, there are additional factors with respect to China's SOEs that increase national security concerns of Foreign Direct Investment (FDI) recipient nations; China's political structure and unique state dominance/control of SOEs presents a different type of investor.[14] China is non-market economy and involved in all critical economic sectors.[15] Describing the Chinese economy, Professor Julien Chaisse of The Chinese University of Hong Kong stated that "[t]he way that the Chinese government exercises 'state capitalism' is that it directly or indirectly controls a large number of powerful SOEs, especially in key strategic sectors."[16]

The *raison d'être* of Chinese SOEs is the advancement of the Chinese Communist Party's (CCP) objectives, thus amplifying the general "state-ownership" concerns. China is ruled by one political party, the CCP, and its domination of Chinese SOEs is of critical importance.[17] The CCP wields near total non-financial control over its citizenry, legislates the law of the land, and appoints judges that interpret its law.[18] These facts are not meant as a criticism of China,

---

[12] *Id.*

[13] *See* BuyRu Ding, *'Public Body' or Not: Chinese State-Owned Enterprise*, J. World Trade 167, 173 (2014).

[14] *See* Guo Shuqing, *The Government's Role in China's Market Economy*, 32 THE CHINESE ECONOMY 26, 31-33 (1999).

[15] *Id*.

[16] *See* Julien Chaisse, *Demystifying Public Security Exception and Limitations on Capital Movement: Hard Law, Soft Law and Sovereign Investments in the EU Internal Market*, 37 U. Pa. J. Int'l L. 583, 594 (2015).

[17] *See* Gabriel Wildau, *China's State-Owned Zombie Economy*, FINANCIAL TIMES (Feb. 29, 2016), https://www.ft.com/content/253d7eb0-ca6c-11e5-84df-70594b99fc47.

[18] *See* KERRY DUMBAUGH & MICHAEL F. MARTIN, CONGRESSIONAL RESEARCH SERVICE, UNDERSTANDING CHINA'S POLITICAL SYSTEM 3-4 (2009).

which has expressed no intent to aggressively advance such goals. Nevertheless, Chinese SOEs may have motivations that align with CCP goals and those aims may not necessarily correlate with other countries' national interests.

While the U.S. government also wishes to advance its geo-political goals, the key distinction is that the U.S. government's pursuit of policies is not necessarily part of private U.S. company investment decision-making. In evaluating FDI from U.S. companies, the presumption is the decision to invest is motivated one-hundred percent by profit. The same cannot be said of Chinese SOE investment. It is thus crucial to internalize that Chinese SOEs related investments may very well harbor an agenda to advance strategic goals for the CCP. These concerns can be expected to grow. The CCP is apparently strengthening its control over SOEs. [19]

The potential motivation to further the goals of an alternative vision of global governance by a private entity investing and buying companies is a very different context for review than traditional corporate acquirers. In addition, investments and joint ventures from SOEs may not be an efficient allocation of resources or profit-generators.[20] If investments are not based upon pure economic motivations, the investments may prove to be less than stellar performers or at a minimum, fail to achieve potential returns. Crucially, such motivations bring potential economic risk and loss of potential into the calculus for a recipient nation.

China has acknowledged the crucial need to reform its inefficient SOEs and that doing so would lend confidence to

---

[19] *See* Kjeld Erik Brødsgaard, *Can China Keep Controlling its SOEs?*, DIPLOMAT (Mar. 5, 2018), https://thediplomat.com/2018/03/can-china-keep-controlling-its-soes/.

[20] *See, e.g.*, *China Says Debt Risk for Main State-Owned Enterprises is Controllable*, BUSINESS TIMES (Jan. 27, 2017), http://economictimes.india times.com/articleshow/56806126.cms?utm_source=contentofinterest& utmmedium=text&utmcampaign=cppst (arguing that while many state companies are bloated and inefficient, China has relied on them more heavily over the past year to generate economic growth in the face of cooling private investment).

recipient nations and lower concerns.[21] However, economic considerations have not trumped political considerations thus far. Rather than utilizing pure economic factors as the benchmark for SOE reform, political factors are considered that may impinge on the profit-making calculus private sector companies engage in.[22] In terms of enacting reforms to China's SOEs, economic performance is surely a factor but not necessarily the controlling factor as it would be in a private sector business.[23] This demonstrates that SOE investment in other countries may potentially be based, at least in part, upon non-economic factors. The fact that some SOEs investments may not have pure economic profit as the driving factor may constitute an inefficient allocation of financial resources and economic potential in addition to raising security concerns.

Although FDI is acknowledged as beneficial and an important enabler of economic vitality, many governments are concerned about the national security implications of FDI.[24] Chinese FDI has come under more stringent scrutiny in recent years sparked by political concerns about foreign ownership in Europe[25]

---

[21] For an excellent discussion of SOE reforms see Leutert, *supra* note 7.

[22] *Id*. at 86 (discussing Beijing's September 2015 release of its long-delayed guiding opinions for reforming state firms, to be followed by a series of policy documents, and noting that three key challenges, block the path ahead: deciding when and how to grant market forces a greater role, especially after stock market turmoil; aligning managerial incentives with firm performance and corporate governance priorities; and overcoming company-level obstacles).

[23] *See* Catherine Tai, *China's Private Sector is Under Siege*, DIPLOMAT (Dec. 22, 2018), https://thediplomat.com/2018/12/chinas-private-sector-is-under-siege/.

[24] *See* Alan P. Larson & David M. Marchick, *Foreign Investment and National Security: Getting the Balance Right*, Council on Foreign Relations CSR No. 18, 4-5 (July 2006).

[25] *See* Keith Johnson & Elias Groll, *As West Grows Wary, Chinese Investment Plummets*, FOREIGN POLICY (Jan. 14, 2019), https://foreignpolicy.com /2019/01/14/chinese-investment-in-the-united-states-and-europe-plummets/ (discussing Chinese firms investing just $30 billion in the United States, Canada, and Europe in 2018, a stark reversal from the $111 billion invested in 2017 and the $94 billion in 2016, and noting that Chinese investment has reinvigorated some sectors, such as European ports, while about 140,000 U.S. jobs are directly provided by Chinese companies).

and the U.S.[26] Some in the U.S. have urged a complete ban on Chinese SOE investment.[27] The U.S. is not alone in signaling a possible reassessment. The EU has also expressed concerns regarding China's FDI into the EU and the associated national security risks of "One Belt, One Road" (OBOR)-driven investment.[28] EU diplomats expressed that "suspicions ran deep over China's geopolitical intentions in Europe, particularly with its massive trade and infrastructure plan, the 'Belt and Road Initiative.'"[29]

On account of these developments, the laws of the U.S. as they relate to foreign investment and national security assume greater importance. The U.S. remains the world's largest net capital importer, attracting more than half of the total Organization of Economic Co-operation and Development inflows.[30] Changes in the content or application of U.S. laws governing foreign investment could, therefore, not only lead other countries to follow, but it could also force significant changes in the flow of FDI worldwide.

The U.S. Treasury Department's Committee on Foreign Investment in the United States (CFIUS) is the primary vetting mechanism in this area.[31] CFIUS wields the power to review a "covered transaction," defined as "any merger, acquisition or

---

[26] *Id*.

[27] *See* Geoff Dyer, *US Urged to Ban Acquisitions by Chinese State-Owned Companies*, FINANCIAL TIMES (Nov. 16, 2016), https://www.ft.com/content/02920e8a-ac48-11e6-ba7d-76378e4fef24.

[28] *See* Philippe Le Corre, *Europe's Mixed Views on China's One Belt, One Road Initiative*, BROOKINGS INST. (May 23, 2017), https://www.brookings.edu/blog/order-from-chaos/2017/05/23/europes-mixed-views-on-chinas-one-belt-one-road-initiative/.

[29] *Id*.

[30] *See* UNCTAD, *World Investment Report* (2018), https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2130 (last visited Dec. 20, 2018) (reporting that the United states has remained the largest recipient of FDI, attracting $275 billion in inflows).

[31] *See* U.S. Dep't of the Treasury, *The Committee on Foreign Investment in the United States (CFIUS)*, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius (last visited June 4, 2019).

takeover … by or with any foreign person which could result in foreign control of any person engaged in interstate commerce in the United States."[32] The term "national security" is not strictly defined and CFIUS focuses on certain strategic national security spheres such as energy, defense, and technology.[33]

The CFIUS review process consists of four steps: (1) a voluntary filing with CFIUS by one or more parties to the transaction; (2) a 30-day Committee review of the transaction; (3) a potential additional 45-day Committee investigation; and (4) within 15 days of receiving the report, the President has to make a decision to permit the acquisition, deny it, or seek divesture after an *ex post facto* review.[34]

For transactions that raise issues, parties may engage in pre-filing consultations and negotiations with CFIUS or member agencies before making their official notification.[35] Although these discussions are not part of the formal CFIUS process, they often influence the outcome.[36] Parties may sometimes modify their transaction before filing to expedite clearance.[37] In other cases,

---

[32] *See* Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons, 31 C.F.R. § 800.401(f) (2008).
[33] *See* 50 U.S.C. App. § 2170 (2001). There are calls to expand the list of areas. *See also* Press Release, Comm. Agric., Nutrition, & Forestry, Senators Stabenow and Grassley Introduce Bipartisan Legislation to Protect American Agricultural Interests in Foreign Acquisitions (Mar. 14, 2017), https://www.agriculture.senate.gov/newsroom/dem/press/release/senators-stabenow-and-grassley-introduce-bipartisan-legislation-to-protect-american-agricultural-interests-in-foreign-acquisitions (proposal to add food security to list).
[34] *See* JAMES K. JACKSON, CONGRESSIONAL RESEARCH SERVICE, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS), 12 (2019).
[35] *See* Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons, 31 C.F.R. § 800.401(f); *see also* EDWARD SHAPIRO ET AL., LATHAM & WATKINS, OVERVIEW OF THE CFIUS PROCESS 5 (2017), https://www.lw.com/thoughtLeadership/overview-CFIUS-process.
[36] *Id*.
[37] *See* Leon B. Greenfield & Perry Lange, *The CFIUS Process: A Primer*, 6 THE THRESHOLD, Winter 2005/2006, at 14.

parties may abandon transactions if it becomes clear that CFIUS will not approve them or will not do so on terms acceptable to the parties.

A CFIUS filing is not mandatory for any transaction. Nevertheless, foreign direct investment by a firm controlled directly or indirectly by a foreign government is subject to mandatory review.[38] The focus of review is directed toward plans for acquiring assets and on national origin i.e. foreign government seeking to engage in any merger, acquisition, or takeover. The CFIUS is required to consider whether the acquisition "could affect national security" rather than applying the "threatens to impair national security" level of scrutiny. The lower standard of review, coupled with the mandatory nature of the inquiry, presents CFIUS with the opportunity to exercise leverage over the acquiring entity or its government.

The 30-day initial review period begins to run once the CFIUS staff gives notice that they are satisfied that the filing contains all of the required information.[39] Although only one party to the transaction need file notice to trigger a review, CFIUS may delay the beginning of the review period until the required information about other parties is received.[40] Thus, CFIUS may, in practice, request a joint filing.[41] During the 30-day initial review, CFIUS may contact the parties for further information or to discuss steps that would mitigate any national security concerns that the transaction raises.

At the end of the 30-day initial review period, CFIUS is required either to clear the transaction based on its initial review or begin an additional 45-day investigation.[42] However, CFIUS may

---

[38] *See* Defense Production Act Extension and Amendments of 1991, Pub. L. No. 102-99, 105 Stat. 487 (1991).
[39] *See* Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, § 1709, 132 Stat. 1287 (2018).
[40] *Id*.
[41] *See* Mario Mancuso et al., *CFIUS Implements New Pilot Program Requiring Submission of Declarations for Certain Transactions*, KIRKLAND ELLIS (Dec. 14, 2018), https://www.kirkland.com/publications/kirkland-alert/2018/12/cfius-implements-new-pilot-program.
[42] *See* 50 U.S.C. § 2170(b) (2012).

informally request that the parties withdraw the filing before the end of the 30-day initial review period if CFIUS needs more time or information to fully review the transaction, or the parties have not agreed to mitigating conditions as requested by agencies.[43] In practice, all presidential administrations since 1992 have considered the 45-day investigation as a "discretionary" option even in cases where a foreign company is government-owned.[44] If the national security concerns raised by a transaction are resolved during the 30-day review, an investigation is not necessary.[45] Therefore, questions arise about what Exon-Florio actually requires,[46] its intent, and whether a 45–day investigations is mandatory.

If CFIUS proceeds with a full investigation of the acquisition, it must conclude its additional review within 45 days.[47] At the conclusion of the investigation, it will submit a recommendation to the President.[48] Normally, CFIUS makes a unanimous recommendation, but if the members are divided they will forward their differing views to the President.[49] The President has 15 days from the date of referral to clear, prohibit, or suspend the acquisition.[50] Action by the President pursuant to CFIUS recommendations is not subject to judicial review.[51] When the

---

[43] *See* Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons, 31 C.F.R. §800.507(a) (2008).
[44] Jonathan C. Stagg, *Scrutinizing Foreign Investment: How Much Congressional Involvement Is Too Much?*, 93 Iowa L. Rev. 325, 337 (2007).
[45] *See* Malkawi, *supra* note 11, at 455.
[46] The Exon-Florio Amendment is the name for CFIUS authorization. See Omnibus Trade and Competitiveness Act of 1988, Pub. L No. 100-418, § 721, 102 Stat. 1107 (1988) (codified at 50 U.S.C. app. § 2170); *see also supra* note 39.
[47] *See* Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons, 31 C.F.R. § 800.401(f).
[48] *Id.* § 800.101.
[49] *Id.* § 800.506(b).
[50] *Id.* § 800.101.
[51] The President's determination is virtually unreviewable. *See* Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, § 6, 121 Stat. 246, 256 (replacing the language in Section 721(d) of the Defense

process reaches the presidential decision stage, the President must report to Congress.[52]

The statutory language of CFIUS provides the timeframe for investigations and recommendations. In total, a CFIUS review may last between 30 and 90 days.[53] However, delays are inherent in the review process. As mentioned above, parties may engage in pre-filing consultations with CFIUS, make a material change to their filing, or file again for the same transaction. Also, CFIUS itself can ask the parties for further information or to withdraw. All these issues can result in extensions and delays in the various stages of the CFIUS review process of a proposed transaction. Parties should engage with the CFIUS early in the process to expedite the process and avoid any delays.

Recent amendments to CFIUS expanded its coverage to include real estate transactions, non-controlling investments in critical technology companies, critical infrastructure companies, and companies that maintain or collect sensitive personal data of U.S. citizens.[54] Some of these new covered areas (personal data, critical infrastructure, and critical technology) seem to specifically

---

Production Act of 1950) (codified as amended at 50 U.S.C. app. § 2170(e)) (slightly amended to add a heading and new numbering by FIRRMA).

[52] *See* Jonathan Wakely & Andrew Indorf, *Managing National Security Risk in an Open Economy: Reforming the Committee on Foreign Investment in the United States*, 9 Harv. Nat'l Sec. J. 1, 10 (2018) (discussing the requirement that the President regularly consult with and report to Congress and annually reaffirm each emergency to avoid automatic termination).

[53] *See* Stephanie Zable, *The Foreign Investment Risk Review Modernization Act of 2018*, LAWFARE (Aug. 2, 2018), https://www.lawfareblog.com/foreign-investment-risk-review-modernization-act-2018.

[54] Other amendments allow parties to covered transactions to file short-form "declarations" instead of a more detailed notice. The amendment also expands CFIUS's review period from 30 to 45 days and allows an investigation to be extended for an additional 15-day period under extraordinary circumstances. *See* U.S. DEP'T OF THE TREASURY, SUMMARY OF FOREIGN INVESTMENT RISK REVIEW MODERNIZATION ACT OF 2018, https://www.treasury.gov/resource-center/international/Documents/Summary-of-FIRRMA.pdf (last visited July 31, 2018).

target Chinese investment.[55] The most important aspect of the recent amendments to CFIUS is that they include language specifically designed for China.[56] This seems to be rare that a regulation would refer to a specific country. The amendment requires the Secretary of Commerce to submit to Congress and CFIUS a biannual report on foreign direct investment transactions made by Chinese entities in the U.S.[57]

Global investment through SOEs is beneficial and necessary to bring economic prosperity worldwide. However, foreign acquisitions of companies can pose a significant challenge for governments. The CFIUS process helps to enhance national security when it identifies specific problems that could threaten U.S. national and economic security and helps resolve these problems while still allowing U.S. business to receive the investment they need. Viewed

[55] *See* Amy Deen Westbrook, *Securing the Nation or Entrenching the Board? The Evolution of CFIUS Review of Corporate Acquisitions*, 102 Marq. L. Rev. 645, 669-71, 679 (2019).
[56] *Id*.
[57] The report will include the total foreign direct investment from China in the U.S.; a breakdown of such investments by value, investment type and government *vs*. non-government investments; a list of companies incorporated in the U.S. through Chinese government investment; information regarding U.S. affiliates of entities under Chinese jurisdiction; an analysis of Chinese investment patterns and the extent to which those patterns align with the objectives of China's Made in China 2025 plan; and other related information. *Id*.; *see* LI XING, *China's Pursuit of the "One Belt One Road" Initiative: A New World Order With Chinese Characteristics*, *in* MAPPING CHINA'S 'ONE BELT ONE ROAD' INITIATIVE, 5-10 (Li Xing ed., Palgrave Macmillan 2019); *see also* Jeffrey N. Gordon & Curtis J. Milhaupt, *China as a "National Strategic Buyer": Toward a Multilateral Regime for Cross-Border M&A*, 19 Colum. Bus. L. Rev. 194 , 223 (2019) (discussing Made in China 2025 ("MIC 2025"), the Chinese government's policy response to challenges facing the country's domestic manufacturing industry, issued by the State Council in May 2015, which identified ten priority sectors accounting for forty percent of China's value-added manufacturing, including next-generation information technology, aviation, new materials, and biosciences).

from this perspective, CFIUS has been successful.[58] In every other country, a CFIUS style review mechanism is an option that should be examined as a potential solution to the upcoming challenges of increasing Chinese investment worldwide. Countries should adopt formal and legal security review of foreign investment to secure legitimate foreign investment and protect strategic sectors from unwanted investment.

[58] *See Examining the Committee on Foreign Investment CFIUS: Hearing Before the S. Comm. on Banking, Housing & Urban Affairs*, 115th Cong. (2017) (statement of James A. Lewis, Ctr. Strategic & Int'l Studies).

POLITICALLY EXEMPT: ANALYSIS OF TURKEY'S FETHULLAH GÜLEN EXTRADITION REQUEST AND U.S. FEDERAL COURT APPLICATION OF THE POLITICAL OFFENSE EXCEPTION

By: Melissa L. Martin[*]

INTRODUCTION

The Republic of Turkey is currently seeking the extradition of Turkish cleric Fethullah Gülen from the United States based upon charges that Gülen orchestrated and commanded Turkey's 2016 coup attempt.[1] The request is pursuant to a bilateral extradition agreement between the U.S. and Turkey.[2] However, under the terms of the treaty, an individual may not be extradited for charges that the Requested Party (herein the U.S.) deems political in nature.[3] The following article examines the *political offense exception* as applied by U.S. federal courts. It then illustrates this application using the publicly available facts regarding the Gülen extradition request to envisage likely outcomes should the request be considered by a U.S. federal court. Section II provides a background summary of the 2016 coup attempt, Gülen's political history and current status, and the extradition request submitted by Turkey to the U.S. Section III provides an overview of extradition agreements generally, the U.S.-Turkey extradition treaty specifically, and the political offense exception to extradition. Section IV examines specific charges against Gülen and applicable U.S. extradition laws. Section V provides concluding remarks.

---

[*] *Juris Doctor*, American University Washington College of Law, 2019. *Master of Arts*, American University School of International Service, 2019.

[1] Mevlut Cavusoglu, *The United States Should Extradite Fetullah Gulen*, FOREIGN POLICY (May 15, 2017), https://foreignpolicy.com/2017/05/15/the-united-states-should-extradite-fetullah-gulen/.

[2] *See* Treaty on Extradition and Mutual Assistance in Criminal Matters, Turk.-U.S., art. 1, June 7, 1979, 3 U.S.T. 3111.

[3] *Id.* art. 3, § 1(a).

The question of Gülen's extradition remains a central point of contention straining relations between the U.S. and Turkey—threatening U.S. national security in the process.[4] Turkey's President Recep Tayyip Erdogan has expressed strong discontent with the U.S. for its failure thus far to extradite and has stated that he would refuse extradition of wanted terrorists to the U.S. until Gülen was repatriated.[5] In addition, the U.S. will rely on Turkey to play a central role in combatting ISIS and securing the Levant once it withdraws troops from the region this spring.[6] Given these circumstances, U.S. foreign policy and national security objectives could be impacted considerably by a court's judgement should the Gülen case ever be passed to the federal judiciary.

I. BACKGROUND

A. *2016 Attempted Turkish Coup*

On the night of July 15, 2016, Turkey experienced the bloodiest coup attempt in its history.[7] A faction of the State's military launched coordinated operations in several major cities to

[4] *See Priorities and Challenges in the U.S.-Turkey Relationship: Hearing Before the S. Comm. On Foreign Relations*, 115th Cong. (Sept. 6, 2017) (testimony of Amanda Sloat, Ph.D., Fellow, Ash Ctr. Democratic Governance & Innovation, Harv. Kennedy Sch.), [hereinafter Sloat testimony], https://www.foreign.senate.gov/hearings/priorities-and-challenges-in-the-us-turkey-relationship_090617.

[5] *Turkey to Halt Extraditions to US Until it Gets Fethullah Gulen*, DEUTSCHE WELLE (Jan. 11, 2018), https://www.dw.com/en/turkey-to-halt-extraditions-to-us-until-it-gets-fethullah-gulen/a-42116304; Julia Harte & Matt Spetalnick, *Turkish Envoy Urges U.S. to Search Cleric Gulen's Communications*, REUTERS, (July 14, 2017), http://news.trust.org/item/20170714230838-vl693.

[6] *See* Sloat testimony, *supra* note 4; *see also* Eric Schmitt, *Trump Seeks to Reassure Anxious Allies On ISIS Fight*, N.Y. TIMES, Feb. 7, 2019, at A12; Dion Nissenbaum & Nancy Youssef, *U.S. Military Sets April Target Date for Leaving Syria*, WALL ST. J., (February 7, 2019), https://www.wsj.com/articles/u-s-military-sets-april-target-date-for-leaving-syria-11549573965.

[7] *Turkey's Failed Coup Attempt: All You Need to Know*, AL JAZEERA, (July 15, 2017), https://www.aljazeera.com/news/2016/12/turkey-failed-coup-attempt-161217032345594.html.

topple the current Turkish government—led by President Erdogan and his Justice and Development Party (AKP).[8] Soldiers took to the streets in tanks, explosions erupted in Istanbul and Ankara, Turkish fighter jets bombed Parliament and the presidential compound, and the chairman of the Joint Chiefs of Staff was abducted by his security team.[9] As news of the coup attempt spread across social media, civilians took to the streets to oppose the coup.[10] With the assistance of loyalist soldiers and police forces, the attempt was quelled within hours.[11] While statistics on casualties vary, approximately 250 civilians are estimated to have been killed and over 2,000 more injured during the failed coup.[12]

President Erdogan and the Turkish government have steadfastly implicated U.S.-based Muslim cleric Fethullah Gülen as the coup's mastermind and architect.[13] They allege that Gülen's followers formed a network within Turkey's military and police sectors and carried out the attempt.[14] Within days of the uprising,

---

[8] *Turkey Timeline: Here's How the Coup Attempt Unfolded*, AL JAZEERA, (July 16, 2016), https://www.aljazeera.com/news/2016/07/turkey-timeline-coup-attempt-unfolded-160716004455515.html.

[9] *Id.*; *see also* Omur Budak, *One Year After Coup Attempt, Turkey is Still Battling Terrorism*, BOS. GLOBE (July 15, 2017), https://www.bostonglobe.com/opinion/2017/07/14/one-year-after-coup-attempt-turkey-still-battling-terrorism/V8BV1hcSJMZdjp6xUyzchM/story.html.

[10] *See Turkey's Failed Coup Attempt: All You Need To Know*, *supra* note 7.

[11] *Id.*

[12] Peter Kenyon, *A Year Later, A Divided Turkey Remembers Failed Coup Attempt*, NPR (July 16, 2017), https://www.npr.org/sections/parallels/2017/07/16/537549673/a-year-later-a-divided-turkey-remembers-failed-coup-attempt.

[13] *Id.*; *see also* Abigail Hauslohner et al., *He's 77, Frail and Lives in Pennsylvania. Turkey Says He's a Coup Mastermind*, WASH. POST (Aug. 3, 2016), https://www.washingtonpost.com/national/hes-frail-77-and-lives-in-pennsylvania-turkey-says-hes-a-coup-mastermind/2016/08/03/6b1b2226-526f-11e6-bbf5-957ad17b4385_story.html?noredirect=on&utm_term=.b9a2496db683.

[14] *Who is Fethullah Gulen, the man Erdogan Blames for Coup Attempt in Turkey?*, CBC (July 21, 2016), https://www.cbc.ca/news/world/fethullah-gulen-profile-1.3686974; Darren Butler, *Turks Believe Cleric Gulen Was Behind Coup Attempt: Survey*, REUTERS (July 26, 2016), https://www.reuters.com/article/us-turkey-security-survey/turks-believe-cleric-gulen-was-behind-coup-attempt-survey-idUSKCN1060P1.

Turkey's top judicial board purged 2,745 judges for alleged Gülen links.[15] As of May 2017, the Turkish government had launched legal proceedings against over 149,000 individuals believed to be aligned with the Gülen movement.[16] Gülen has publicly denounced the coup and denied having any prior knowledge of or part in the uprising.[17] Turkey is currently seeking Gülen's extradition from the U.S. based upon charges stemming from the attempted coup—as well as several charges pre-dating the coup.[18]

B. *Gülen and Erdogan – Allies to Adversaries*

Gülen and President Erdogan have a storied past, which has given the extradition request a distinctly political air and led many to accuse Erdogan of scapegoating Gülen in order to consolidate power.[19] Gülen was once a close political ally of Erdogan's, assisting the AKP in democratizing Turkey and ending military

---

[15] Emre Peker & Carol E. Lee, *U.S., Turkey on Collision Course Over Ankara's Demand for U.S.-Based Cleric*, WALL ST. J. (July 16, 2016), https://www.wsj.com/articles/turkish-president-says-u-s-exile-fethullah-gulen-responsible-for-coup-1468693543.

[16] *Justice Minister in US over Gulen's Extradition Demand*, HURRIYET DAILY NEWS (May 6, 2017), http://www.hurriyetdailynews.com/justice-minister-in-us-over-gulens-extradition-demand-112795.

[17] Tom O'Conner, *Who is Fethullah Gulen? Turkey Links Muslim Cleric to Murder of Russian Ambassador*, INT'L BUS. TIMES (Dec. 20, 2016), https://www.ibtimes.com/who-fethullah-gulen-turkey-links-muslim-cleric-murder-russian-ambassador-2463424.

[18] Dominic Evans, *Turkey's Erdogan Links Fate of Detained U.S. Pastor to Wanted Cleric Gulen*, REUTERS (Sept. 28, 2017), https://www.reuters.com/article/us-usa-turkey-cleric/turkeys-erdogan-links-fate-of-detained-u-s-pastor-to-wanted-cleric-gulen-idUSKCN1C31IK; Karen DeYoung, *Turkish Evidence for Gulen Extradition pre-dates Coup Attempt*, WASH. POST (Aug. 19, 2016), https://www.washingtonpost.com/world/national-security/turkish-evidence-for-gulen-extradition-pre-dates-coup-attempt/2016/08/19/390cb0ec-6656-11e6-be4e-23fc4d4d12b4_story.html?utm_term=.893b0e26f9ec.

[19] *See, e.g.*, Ishaan Tharoor, *Turkey's Erdogan Turned a Failed Coup into his Path to Greater Power*, WASH. POST (July 17, 2017), https://www.washingtonpost.com/news/worldviews/wp/2017/07/17/turkeys-erdogan-turned-a-failed-coup-into-his-path-to-greater-power/?utm_term=.87e12cb50f51.

influence in Turkish politics. [20] Gülen is alleged to have re-staffed the bureaucracy with his supporters in the process.[21] Yet by 2013, the alliance had been fractured by a string of police raids on and investigations into key AKP members and associates—allegedly carried out by officers loyal to Gülen.[22]

Formally named *Hizmet*, the Gülen movement is reportedly the largest Muslim network in the world.[23] There are purportedly several million Gülen followers in Turkey and up to seven million more worldwide.[24] The movement claims to promote a tolerant view of Islam and to encourage altruism, modesty, and education.[25] Hizmet has established charter schools throughout the world—many located in the U.S. and Europe—which educate nearly 2 million children.[26]

Critics of Hizmet accuse the movement of questing to gain power in order to spread a socially conservative brand of Islam worldwide.[27] Deemed the *Fethullah Gülen Terrorist Organization* (FETO) by the Turkish government, Hizmet has been designated as a terrorist group within Turkey.[28] Despite this designation, and the fact that Gülen has dwelled in secluded Saylorsburg, Pennsylvania for nearly two decades, many regard him as Turkey's second most

---

[20] *See Turkey's Failed Coup Attempt: All You Need to Know*, *supra* note 7; *see also* Peker, *supra* note 15.
[21] *See Turkey's Failed Coup Attempt: All You Need to Know*, *supra* note 7.
[22] *See Turkey Timeline: Here's How the Coup Attempt Unfolded*, *supra* note 8.
[23] *Profile: Fethullah Gulen's Hizmet Movement*, BBC (Dec. 18, 2013), https://www.bbc.com/news/world-13503361.
[24] *Id.*; *see also* Scott Beauchamp, *120 American Charter Schools and One Secretive Turkish Cleric*, THE ATLANTIC (Aug. 12, 2014), https://www.theatlantic.com/education/archive/2014/08/120-american-charter-schools-and-one-secretive-turkish-cleric/375923/.
[25] *Profile: Fethullah Gulen's Hizmet Movement*, *supra* note 23; *see also Turkey coup: What is Gulen Movement and What Does it Want?*, BBC (July 21, 2016), https://www.bbc.com/news/world-europe-36855846.
[26] Beauchamp, *supra* note 24.
[27] *Profile: Fethullah Gulen's Hizmet Movement*, *supra* note 23.
[28] Dylan Matthews, *Turkey's Coup: the Gulen Movement, Explained*, VOX (Sept. 13, 2016), https://www.vox.com/2016/7/16/12204456/gulen-movement-explained.

powerful man given his expansive network and following—eclipsed in status only by Erdogan him.[29] Considering the power dynamics intrinsic to the Erdogan-Gülen relationship, the U.S. faces a particularly precarious diplomatic challenge as it considers Turkey's extradition request.

C. *Turkey's Extradition Request*

On September 12, 2016, the Turkish Justice Ministry submitted its first request to the U.S. for the extradition of Fethullah Gülen based on the findings of a Turkish judicial investigation into the coup attempt.[30] The charges against Gülen reportedly include ordering and commanding a coup attempt, attempt to overthrow the government, terrorism, and acts against a head of State.[31] (The Turkish government submitted a prior extradition request for Gülen in July 2016, shortly before the coup attempt at issue took place; the request was premised upon four charges—including attempt to overthrow the government—for which Gülen was being tried *in absentia*.[32] For the sake of concision, this analysis focuses only on those charges stemming from the 2016 coup attempt.)

Since the extradition request for Gülen was issued, it has laid largely dormant. While U.S. State Department officials are still considering the request with the help of the Department of Justice, sufficient evidence has not been provided to refer the request to a U.S. district judge or magistrate judge.[33] As is the case with all

---

[29] *See Profile: Fethullah Gulen's Hizmet Movement*, *supra* note 23.
[30] *See* Cavusoglu, *supra* note 1.
[31] *See* Mathews, *supra* note 28; Adam Withnall & Samuel Osborne, *Erdogan Blames 'foreign powers' for Coup and Says West is Supporting Terrorism*, INDEPENDENT (Aug. 2, 2016), https://www.independent.co.uk/news/world/europe/erdogan-turkey-coup-latest-news-blames-us-west-terrorism-gulen-a7168271.html; Kubra Chohan & Sena Guler, *Turkey Says US Bound by Treaty to Extradite Gulen*, ANADOLU AGENCY (Oct. 19, 2017), https://www.aa.com.tr/en/politics/turkey-says-us-bound-by-treaty-to-extradite-gulen/941826.
[32] Matthews, *supra* note 28; Peker, *supra* note 15.
[33] *See* Katheryn Watson, *State Department Says U.S. is Evaluating Turkish Materials on Fethullah Gulen*, CBS NEWS (Nov. 16, 2018), https://www.

extradition requests, Turkey must present preliminary evidence to the U.S. Department of State demonstrating probable cause that a crime was committed.[34] If and when sufficient evidence is presented, the extradition request will be referred to a U.S. federal court for a probable cause hearing.[35] Turkey has reportedly failed thus far to provide satisfactory evidence warranting the request's referral to a federal court.[36] President Erdogan has expressed strong discontent with the U.S. for its failure to extradite—stating that he would refuse extradition of wanted terrorists from Turkey to the U.S. until Gülen was repatriated.[37] Turkey is reportedly working to gather and present additional evidence against Gülen at this time.[38]

Notwithstanding these preliminary challenges, the Turkish government faces an uphill battle in securing Gülen even upon a showing of sufficient evidence implicating Gülen. Turkey will have to demonstrate that the charges against Gülen do not fall under a major caveat to the U.S.-Turkey extradition treaty: the political offense exception. As this article illustrates, the exception protects individuals like Gülen who have been charged with crimes deemed

---

cbsnews.com/news/state-department-says-u-s-is-evaluating-turkish-materials-about-fethullah-gulen/; *see also* 18 U.S.C. § 3184 (2012) (establishing that any justice, judge, or magistrate judge for the United States may consider evidence of a foreign fugitive's criminality).

[34] Michael Werz & Max Hoffman, *The Process Behind Turkey's Proposed Extradition of Fethullah Gulen*, CTR. FOR AM. PROGRESS (Sept. 7, 2016), https://www.americanprogress.org/issues/security/reports/2016/09/07/143587/the-process-behind-turkeys-proposed-extradition-of-fethullah-gulen/.

[35] *See* 18 U.S.C. § 3184.

[36] *See* Erin Cunningham, *U.S. Officials in Turkey to Discuss Extradition of Exiled Cleric, State Media Says*, WASH. POST (Jan. 3, 2019), https://www.washingtonpost.com/world/us-officials-in-turkey-to-discuss-extradition-of-exiled-cleric-state-media-says/2019/01/03/00197348-4f34-48d8-ad53-abe5a0167a53_story.html?noredirect=on&utm_term=.4ca17bc13167.

[37] *Turkey to Halt Extraditions to US Until it Gets Fethullah Gulen*, *supra* note 5; Harte & Spetalnick, *supra* note 5.

[38] Chohan & Guler, *supra* note 31.

political in nature.[39] The exception would almost certainly be raised as a defense to each of the charges against Gülen, and the situation therefore presents a valuable case study to examine the federal judiciary's interpretation of this universally recognized exception to extradition.

III. EXTRADITION AGREEMENTS

A. Extradition History and U.S. Procedure

Extradition is the process by which a jurisdiction secures the return of a suspected or convicted criminal from another jurisdiction.[40] The principle of State sovereignty, recognized as a fundamental State right under international law, affords each State the right to control all persons within its territory.[41] As such, a State has no duty to extradite individuals within its borders who commits a crime in a foreign jurisdiction.[42] However, many States opt to undertake this duty—a slight cession of sovereignty—in order to enjoy reciprocal treatment from other States.[43]

Increased international mobility and migration, particularly after the Industrial Revolution, resulted in the widespread international movement of criminals hoping to evade justice—and a desire by States to secure their return.[44] States began to forge bilateral treaties on extradition to accomplish this objective. These extradition agreements initially targeted individuals who had

---

[39] David M. Lieberman, *Sorting the Revolutionary from the Terrorist: The Delicate Application of the "Political Offense" Exception in U.S. Extradition Cases,* 59 STAN. L. REV. 181, 183 (2006).
[40] MALCOLM N. SHAW, INTERNATIONAL LAW 422 (1991).
[41] *Id.*
[42] *Id.*
[43] For example, over 100 nations have signed extradition treaties with the U.S. *See* 18 U.S.C. § 3181 (2012).
[44] Stuart Phillips, *The Political Offense Exception and Terrorism: Its Place in the Current Extradition Scheme and Proposals for Its Future,* 15 DICKINSON J. INT'L L. 337, 339 (1997).

committed common crimes such as rape, murder, and theft.[45] Over time, however, extradition agreements have broadened to cover a host of violations agreed upon by the State parties. Today, these bilateral treaties generally oblige their signatories to return individuals who have committed any act that constitutes a crime in both the Requesting State and the Requested State—a concept known as *dual criminality*.[46]

In the U.S., the executive and judicial branches share extradition powers.[47] As noted above, the Department of State serves as the gatekeeper to extradition, requiring a preliminary determination that probable cause of a crime may be found based upon the evidence provided. Once a federal judge receives an extradition request, (s)he must make several determinations: (1) whether (s)he is authorized to conduct the proceeding; (2) whether the court has jurisdiction over the individual; (3) whether the applicable treaty is in full force and effect; (4) whether the alleged crimes fall within the scope of the treaty; and (5) whether probable cause exists to believe that the individual charged committed the alleged crime(s).[48] If the court finds that probable cause exists, the Secretary of State retains final discretion to decide whether the fugitive will be returned to the Requesting State.[49]

---

[45] *Id.*

[46] The concept of dual criminality is a requirement for extradition, recognized in virtually every bilateral extradition treaty. It requires that the offense charged be considered a crime in both the Requesting State and the Requested State. A dual criminality clause is included in the United Nation's Model Treaty on Extradition. *See* Jonathan O. Hafen, *International Extradition: Issues Arising Under the Dual Criminality Requirement*, 1992 BYU L. Rev. 191, 191 (1992).

[47] *See* 18 U.S.C. § 3184.

[48] Lieberman, *supra* note 39, at 187 (citing *In re* Atuar, 300 F. Supp. 2d 418, 425-26 (S.D. W. Va. 2003)).

[49] *See* 18 U.S.C. § 3186; *cf. In re* Sindona, 450 F. Supp. 672, 694 (S.D.N.Y. 1978) ("[t]he Department of State has the discretion to deny extradition on humanitarian grounds, if it should appear that it would be unsafe to surrender [the fugitive] to the [requesting state].").

B. U.S.-Turkey Extradition Treaty

The extradition treaty between the U.S. and Turkey forms the legal basis for Turkey's extradition request. The "Treaty on Extradition and Mutual Assistance," signed in Ankara on June 7, 1979, is unexceptional—containing standard clauses regarding extradition and incidents of exception. Article 1 obliges the Requested Party to surrender to the Requesting Party—in accordance with the provisions and conditions of the Treaty—all persons who are found within the Requested Party's territory and who have been charged with or convicted of an offense committed within the territory of the Requesting Party.[50] Article 2 defines extraditable offenses as offenses which are punishable under both the federal laws of the U.S. and the laws of Turkey (dual criminality) by deprivation of liberty for a period at least exceeding one year or by a more severe penalty.[51] Significant to this article's analysis, the act of *attempting* or *conspiring* to commit—or participating as principal, accomplice, or accessory in—any extraditable offense is an extraditable offense under Article 2.[52]

Article 3 establishes the political offense exception, stating that extradition shall not be granted:

> (a) If the offense for which extradition is requested is regarded by the Requested Party to be of a political character or an offense connected with such an offense; or if the Requested Party concludes that the request for extradition has, in fact, been made to prosecute or punish the person sought for an offense

[50] Treaty on Extradition and Mutual Assistance in Criminal Matters, Turk.-U.S., art. 1, June 7, 1979, 3 U.S.T. 3111.

[51] *Id.*, art. 2, § 1(a). Note: The treaty also permits extradition for the State crimes of kidnapping, abduction, false imprisonment, and child-stealing when such crimes are punishable under both U.S. and Turkish law by deprivation of liberty for at least a period exceeding one year or by a more severe penalty. *See* Treaty on Extradition and Mutual Assistance in Criminal Matters, Turk.-U.S., art. 2, § 1(b), June 7, 1979, 3 U.S.T. 3111.

[52] *Id.*, art. 2, § 3(a)-(b).

> of a political character or on account of his political opinions.

Treaty on Extradition and Mutual Assistance, Turkey-U.S., art. 3, § 1(a). Importantly, any offense committed or attempted against a head of State, a head of government, or against a member of his or her family shall not be deemed a political offense.[53] The right to determine the nature of the offense, which entails the granting or refusal of extradition, rests solely with the Requested Party.[54]

C. History of the Political Offense Exception

The political offense exception shields from extradition individuals who face criminal prosecution in the Requesting State for offenses deemed political in nature.[55] There exists a strong international consensus as to its validity,[56] and the exception is expressly included in virtually every modern extradition agreement.[57] Yet, despite near universal acceptance of the exception, there exists little consensus among States as to what acts constitute a political offense. In the U.S., the federal judiciary attempted to craft a framework for the political offense analysis that—for a time—promoted clarity, uniformity, and above all objectivity in decisions.[58] Yet, as demonstrated below, subsequent decisions reinterpreting this once-clear framework have injected a subjective element into the traditionally objective analysis, undercutting (perhaps for good reason) the traditional objective of the political offense exception to shield foreign revolutionaries no matter their political persuasion.

---

[53] *Id.* art. 3, § 1(a).
[54] *Id.* art. 5.
[55] Lieberman, *supra* note 39, at 183.
[56] *Id.*
[57] Phillips, *supra* note 44, at 340.
[58] *See, e.g.*, Sindona v. Grant, 619 F.2d 167, 173 (2d Cir. 1980) ("[f]ollowing the principle announced in *In re Castioni,* American courts have uniformly construed 'political offense' to mean those that are incidental to severe political disturbances such as war, revolution and rebellion.") (internal citation omitted).

The practice of immunizing political fugitives from extradition gained widespread international support as a result of the eighteenth century's prevailing revolutionary ideology.[59] In this century, States witnessed a period of rapid political transformation—and a rise in crimes committed against the State spurred by revolutionary aims.[60] Nations including the U.S. were put in the precarious position of determining whether to turn over revolution instigators for prosecution—often by governments seeking political retribution.[61] Facing this dilemma, States were largely persuaded by the revolutionary ideology emerging in Western society at the time, which championed the ideals of freedom, democracy, and rebellion against oppression.[62] This ideology was the justification for both the French and American revolutions.[63] And while revolutionary activities such as attempt to overthrow of the government were (and remain) federal crimes in the U.S.,[64] the fundamental concept underlying the nation's inception was the right of the people to revolt against tyranny.[65] Indeed, the U.S. Declaration of Independence states, *"*When a long train of abuses and usurpations, pursuing invariably the same Object, evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security."[66] The U.S. thus chose and continues to give deference to this right by refusing the extradition of fugitives seeking to accomplish similar revolutionary aims abroad—regardless of whether the U.S. government agrees with their political objectives.[67]

The political offense exception has never been codified via domestic statute in the U.S.; however, the federal courts have

[59] Lieberman, *supra* note 39, at 186.
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] 18 U.S.C. § 2385.
[65] Lieberman, *supra* note 39, at 186.
[66] *See* THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776).
[67] Lieberman, *supra* note 39, at 186.

adopted a framework in order to ensure its protections. First, courts have recognized a distinction between *pure* and *relative* political offenses.[68] A pure political offense is an action directed solely at the State that does not have any elements of a common crime.[69] Pure offenses include crimes such as treason, sedition, conspiracy to overthrow the government, and espionage.[70] Within the international community, there seems to be unanimous agreement as to the exception of these offenses to extradition.[71]

In contrast, a relative political offense is a crime of a hybrid nature, which either involves a combination of a common crime and a pure political offense or a common crime that is executed in pursuit of a political objective.[72] There is no universal agreement within the international community—nor, it appears, within the U.S. federal judiciary—as to what constitutes a relative political offense. However, the federal courts have attempted for years to craft a workable test to utilize in their analysis of such offenses. This test, known as the *incidence test*, was in fact first established in the 1894 British case *In re Castioni.*[73] The Court in *Castioni* defined a political offense as a crime "incidental to and forming a part of a political disturbance."[74] The test was first applied in the U.S. three years later by a District Court in *In re Ezeta* and was later adopted by the Supreme Court in *Ornelas v. Ruiz*.[75] U.S. federal courts have

---

[68] Phillips, *supra* note 44, at 341.
[69] M. BASSIOUNI, INTERNATIONAL EXTRADITION AND WORLD PUBLIC ORDER 379 (1975).
[70] *Id*. at 380.
[71] *See, e.g.*, Chandler v. United States, 171 F.2d 921 (1st Cir. 1948), *cert. denied*, 336 U.S. 918 (1949) (allowing a prosecution for treason, but noting that extradition could have been refused); *ex parte* Kolczynski, 1 Q.B. 540 (1954) (refusing to extradite mutineers from a Polish vessel); Alfred E. Novotne, *Random Bombing of Public Places: Extradition and Punishment of Indiscriminate Violence Against Innocent Parties*,6 B.U. INT'L. L. J. 219, 230 (1988).
[72] *See* C. VAN DEN WIJNGAERT, THE POLITICAL OFFENSE EXCEPTION TO EXTRADITION 108 (1980).
[73] Lieberman, *supra* note 39, at 187.
[74] *In re* Castioni, [1891] I Q. B. 149.
[75] Lieberman, *supra* note 39, at 187.

traditionally enforced the two-pronged incidence test to determine whether an act that is not "pure" should nonetheless be deemed political in nature.[76]

Each prong of the incidence test must be fulfilled for a crime to qualify as a relative political offense and therefore non-extraditable. First, it must have occurred during a political revolt, disturbance, or uprising.[77] In their analyses, courts look for a requisite level of violence within the State where the offense occurred.[78] Second, the act must be incident to or having formed a part of the uprising. This prong eliminates crimes occurring during a political uprising yet unrelated to it from being protected by the political offense exception—for example, looting a store while an uprising is ongoing.[79] It aims to shield individuals who have committed offenses to both advance a political revolution as well as to quell one.[80]

Unorthodox methods of warfare emerging in the 1970s and 1980s—and particularly the dramatic increase in international terrorism—resulted in an influx of individuals invoking the political offense exception, forcing courts to re-examine the incidence test.[81] Yet in the judiciary's effort to adapt, it made the political offense exception untenable.[82] Courts began to either limit or broaden the two prongs of the incidence test in order to reach a specific result—creating a situation wherein a judge must choose between strict

---

[76] *See* Sindona v. Grant, 619 F.2d 167, 173 (2d Cir. 1980).
[77] *See* Quinn v. Robinson, 783 F.2d 776, 797 (9th Cir. 1986); Eain v. Wilkes, 641 F.2d 504, 518 (7th Cir. 1981); Garcia-Guillern v. United States, 450 F.2d 1189, 1192 (5th Cir. 1971).
[78] *See, e.g.*, *Quinn*, 783 F.2d at 807 ("[E]xception [is] applicable only when a certain level of violence exists and when those engaged in that violence are seeking to accomplish a particular objective.").
[79] *In re* Doherty, 599 F. Supp. 270, 277 n.7 (S.D.N.Y. 1984); *see also* Omelas v. Ruiz, 161 U.S. 502, 511-12 (1896).
[80] Koskotas v. Roche, 931 F.2d 169, 172 (1st Cir. 1991).
[81] Lieberman, *supra* note 39, at 191.
[82] *Id.* at 200.

neutrality or making a value judgement as to the proper course of a revolution.[83]

One response from courts to the swell of unorthodox political offense claims was to administer strict neutrality in their analysis. Judges declined to give any weight to the wisdom of the conduct, so long as said conduct was incidental to and forming a part of an uprising.[84] These decisions followed strictly the holding of the Court in *In re Ezeta*, wherein the Court claimed to have no authority to judge what acts were within the rules of civilized war.[85] The *Ezeta* Court opined that "crimes may have been committed by the contending forces of the most atrocious and inhuman character, and still the perpetrators of such crimes escape punishment as fugitives beyond the reach of extradition."[86] Such was the general contention of federal courts through the mid-1980s. This appeal to neutrality allowed for principled and consistent application of the political offense exception. In turn, however, it prevented the courts from making more nuanced decisions based on the strength of an individual's political motives and the legitimacy of his tactics.[87] During this period until 1986, for example, every member of the Irish Republican Army (IRA)—a U.K.-designated terrorist organization—who claimed protection from extradition under the political offense exception succeeded in the U.S..[88]

---

[83] *Id.*; *see also* Nancy M. Green, *In the Matter of the Extradition of Atta: Limiting the Scope of the Political Offense Exception*, 17 BROOK. J. INT'L L. 447, 463 (1991).

[84] *See* Lieberman, *supra* note 39, at 191 (citing Sindona v. Grant, 619 F.2d 167, 173 (2d Cir. 1980); Garcia-Guillem v. United States, 450 F.2d 1189, 1192 (5th Cir. 1971); *In re* Mackin, No. 80 Cr. Misc. 1, 1981 U.S. Dist. LEXIS 17746, at* 31-40 (S.D.N.Y. Aug. 13, 1981); *In re* Gonzalez, 217 F. Supp. 717, 720-21 (S.D.N.Y. 1963); Ramos v. Diaz, 179 F. Supp. 459, 462-63 (S.D. Fla. 1959)).

[85] *In re* Ezeta, 62 F. 972, 997 (N.D. Cal. 1894) ("I have no authority, in this examination, to determine what acts are with the rules of civilized warfare, and what are not. War, at best, is barbarous . . .").

[86] *Id.*

[87] *See* Lieberman, *supra* note 39, at 194.

[88] *Id.*

Seeking reform, courts forged alternative approaches to reach more intuitive conclusions regarding extradition. The Seventh Circuit in *Eain v. Wilkes* concocted a test balancing the means and ends of acts harming civilians in their extradition determination while addressing an extradition request for a Palestine Liberation Organization (PLO) member accused of bombing an Israeli marketplace.[89] The Court ruled that even if a political uprising were in progress when the Defendant carried out the bombing, only actions that disrupt the political structure of the State and not its social structure would be considered incidental to the goal of toppling the government absent a direct link between the perpetrator, a political organization's political goals, and the specific act.[90] The Court thus found the PLO fugitive to be extraditable based upon the nature of his conduct.

While the Court in *Eain* reached what many would deem the morally correct outcome, the precedent established by this decision has taken the traditionally objective incidence test and injected a subjective element into it. Despite the crimes in *Eain* being offenses committed in a clear effort to undermine or propel reform within the Israeli government, the Court's decision essentially recognized the authority of judges to subjectively analyze an offense's resultant impact in situations where courts have long attempted to remain objective and neutral—particularly given the inherently political nature of the acts. This standard of analysis is particularly problematic when considering acts of unconventional modern warfare, wherein harm to society is used as a method of political change.[91] Despite its challenges, many courts follow the *Eain* analysis. Others have made rulings based upon additional findings as to what constitutes a political offense. The Fourth Circuit adopted the *Eain* Court's finding in *Ordinola v. Hackman*.[92] The Second Circuit similarly held in *Ahmad v. Wigen* that offenses transcending

[89] Eain v. Wilkes, 641 F.2d 504, 507 (7th Cir. 1981).

[90] *Id*. at 521.

[91] *See* Lieberman, *supra* note 39, at 195.

[92] Ordinola v. Hackman, 478 F.3d 588 (4th Cir. 2007).

the law of armed conflict are beyond the limited scope of the political offense exception to extradition.[93] The District Court for the Eastern District of California held in *In re Extradition of Singh* that the political offense exception quite simply does not apply to charges of domestic terrorism.[94]

Courts have also carved out categorical restraints to the traditional incidence test—creating objective but rigid limitations that have failed to prove sufficiently workable in a broad number of cases.[95] These have included, for example, geographic limitations. The Ninth Circuit in *Quinn v. Robinson* defined an uprising as "a revolt by indigenous people against their own government or an occupying power."[96] Therefore, the Court found that an IRA member was extraditable for alleged offenses against and in the sovereign territory of England, as no uprising by its indigenous people was occurring at the time of the alleged act.[97] Likewise, in *In re Extradition of Suarez-Mason*, a California district court found that the political offense exception does not apply to government officials.[98]

These interpretations of the political offense exception evidence a shift away from the neutral, strict application of the two-pronged incidence test into a murky and oft subjective realm of analysis that varies by circuit. While the policy objectives behind this shift are self-evident and highly persuasive, they nonetheless serve to obfuscate the definition and bounds of the political offense exception as established by the Supreme Court in *Ornelas*. Moreover, they serve to undercut the original intent of the political offense exception to shield foreign revolutionaries from persecution, regardless of whether the U.S. government condones their cause. Having briefly examined the current state of the political offense

---

[93] Ahmad v. Wigen, 910 F.2d 1063 (2d Cir. 1990), *affirming* Ahmad v. Wigen, 726 F. Supp. 389 (E.D.N.Y. 1989).
[94] *In re* Extradition of Singh, 170 F. Supp. 2d 982 (E.D. Cal. 2001).
[95] *See* Lieberman, *supra* note 39, at 197.
[96] 783 F.2d 776, 803 (9th Cir. 1986).
[97] *Id.*
[98] *In re* Suarez-Mason, 694 F. Supp. 676 (N.D. Cal. 1988).

exception in the U.S., we now turn toward examining specific reported charges levied against Gülen by the Republic of Turkey and the potential result the political offense exception will have on Turkey's bid for extradition given its modern application.

IV. CHARGES AND APPLICABLE U.S. LAW

Reports allege that the Turkish government seeks to extradite Fethullah Gülen from the U.S. for multiple offenses, including ordering and commanding the July 2016 coup attempt, commanding an armed terrorist organization to commit acts of terrorism, and ordering the assassination of President Recep Tayyip Erdogan.[99] The specific charges and evidence communicated by Turkey to the Department of State are not publicly disclosed. However, this analysis assumes arguendo that the allegations against Gülen have merit in order to assess likely judicial application of the political offense exception to a relevant fact pattern.

The offenses for which Gülen has reportedly been charged—conspiring to overthrow the government, attempt to overthrow the government, commanding an armed terrorist organization, and ordering an assassination of a head of State—are all crimes in both Turkey and the U.S. punishable by at least one year's prison time or a more serious punishment.[100] As such, they are extraditable offenses unless a U.S. federal court finds an applicable exception.[101] This section considers whether each individual charge would withstand scrutiny under the political offense exception as applied by U.S. federal courts.

---

[99] Matthews, *supra* note 28; Fevzi Kizilkoyun, *Gulen Ordered Followers to Conceal Themselves After December 2013 Probes: Report*, HURRIYET DAILY NEWS (Mar. 9, 2017), http://www.hurriyetdailynews.com/gulen-ordered-followers-to-conceal-themselves-after-december-2013-probes-report---110612; Chohan & Guler, *supra* note 31.

[100] *See* 18 U.S.C. §§ 2385, 2339A, 1751 (2012); *see also* CODE PENAL art. 307, 310, 312, (Turk.).

[101] *See* Treaty on Extradition and Mutual Assistance, Turkey-U.S., art. 2, § 1(a), June 7, 1979, 3 U.S.T. 3111.

A. Conspiracy and Attempt to Overthrow the Government

As noted above, conspiracy and attempt to overthrow one's government are universally recognized pure political offenses, protected from extradition under the political offense exception.[102] Unlike relative political offenses, pure political offenses are not subject to the incidence test. Consequently, these offenses do not have to occur incident to or form a part of an uprising. The reasoning behind this distinction is self-evident: Applying the incidence test to such crimes would undercut the very policy that led to the political offense exception's inception—the right of the people to revolt against tyranny. It is quite illogical to shield from extradition individuals who committed a political offense *during* an uprising against tyranny, while leaving the individuals most at risk—those who *instigated* the uprising—subject to extradition because their political scheming preceded the subsequent uprising.

As such, conspiracy by a foreign national to overthrow his home government is a charge largely, if not entirely, un-adjudicated in U.S. federal courts.[103] Any extradition requests predicated upon such a pure political offense would generally hold no potential for extradition under the exception. Additionally, no law exists in the U.S. expressly prohibiting foreign nationals from instigating an uprising against their home governments—so long as they are not linked to terrorism. Notably, another seldom adjudicated crime—the waging of war by a U.S. citizen against a nation at peace with the U.S.—*is* expressly prohibited under U.S. law by the Neutrality Act of 1794.[104] However, no comparable law exists for foreign nationals residing in the U.S.. Thus, the charge of conspiracy to

---

[102] Phillips, *supra* note 44, at 342.

[103] Several courts have considered extradition requests wherein conspiracy to overthrow the government was charged, but these cases were decided on other grounds.

[104] Neutrality Act of 1794, 18 U.S.C. § 958; *see also Coup Attempt in The Gambia*, FBI (Oct. 13, 2017), https://www.fbi.gov/news/stories/coup-attempt-in-the-gambia.

overthrow the government of Turkey alleged against Gülen has no apparent consequence in the U.S.—whether by extradition or domestic prosecution.

B. Terrorism

Unlike conspiracy and attempt to overthrow the government, terrorism is not considered a pure political offense. Indeed, many would seek to have it stricken from the list of relative political offenses. Nevertheless, acts of terrorism have fallen both inside and outside of the political offense exception's parameters depending on whether the presiding judge follows the neutral incidence test or injects additional analyses into their ruling. (Notably, the U.S. has not amended its extradition treaty with Turkey exempting violent crimes such as terrorism from the protection of the political offense exception like it has with other States.[105] Thus, these acts will be considered under the framework of the political offense exception by courts.)

What is clear from the breadth of court opinions on matters regarding terrorism as a political offense is that no consistent rule exists. While a trend toward excluding acts of terrorism from the exception is evident, the line in the sand differentiating unprotected acts of terrorism from political offenses that have caused civilian harm varies greatly dependent upon facts of the crime, jurisdiction, and indeed upon the presiding judge's individual discretion. This variance, created by deviations from the traditional incidence test, is a decided challenge to formulating outcome predictions regarding Turkey's extradition request. This is particularly true considering the fact that the specific acts carried out during the coup, which Gülen allegedly commanded, fail to strike observers as

[105] Responding to increased invocation of the political offense exception by individuals accused of terrorism-related charges (particularly stemming from the conflict in North Ireland), the U.S. and the U.K. signed a Supplementary Treaty exempting number of violent crimes from the political offense exception's umbrella. Antje C. Petersen, *Extradition and the Political Offense Exception in the Suppression of Terrorism*, 67 IND. L. J. 767, 767 (1992).

indiscriminate acts of terror against civilians. Even assuming the Turkish government can definitively link Gülen to the acts carried out by coup participants in the 2016 uprising, coups are—frankly—seldom bloodless and generally accrue unintended civilian casualties while being carried out. In contrast to the indiscriminate bombings addressed in cases like *Eain*, the Turkish military in its long history of coup instigation has generally carried out its revolutionary activities with precision—limiting its aims to deposing the current government pursuant its duties under the Turkish Constitution.[106] Thus, whether specific offenses charged in the Gülen case will be deemed terrorism or simply rebellion is a question to be determined by the court tasked with administering a probable cause hearing. Considering the range of prior rulings on like scenarios, this determination will likely depend on a combination of the facts, jurisdictional precedent, and a dose of individual discretion on the part of the judge.

Importantly, there exist a number of international conventions to which both Turkey and the U.S. are parties that expressly permit the extradition of criminals for terror-related offenses. Of these, the International Convention Against the Taking of Hostages stands out as most relevant to the Gülen scenario. This particular Convention necessitates extradition or prosecution of any individual who has committed, attempts to commit, or acts as an accomplice to anyone who commits or attempts to commit "hostage-taking."[107] According to the Convention, hostage-taking is committed by any person who seizes or detains and threatens to kill, injure, or continue to detain another person in order to compel a third party (herein the State) to do or abstain from doing any act as an

[106] Turkey's constitution gives the military authority to step in when democracy or human rights are threatened. Daphne Caruana Galizia, *Under the Turkish Constitution, the Army is Obliged to Step in When the Democratically-Elected Government Behaves Undemocratically*, RUNNING CONTEMPORARY (July 16, 2016, 3:36 PM), https://daphnecaruanagalizia.com/2016/07/84059/.

[107] Int'l Convention Against the Taking of Hostages art. 1, § 1, Dec. 19, 1979, 1316 U.N.T.S. 205.

explicit or implicit condition for the release of the hostage.[108] In addition to the alleged attempted kidnapping of President Erdogan—discussed below—the chairman of Turkey's Joint Chiefs of Staff, Hulusi Akbar, was reportedly kidnapped and detained by his own security detail during the 2016 coup attempt.[109] He was rescued the following day.[110] In his testimony, Akbar claimed that his abductors offered him a chance to speak to Gülen over the phone while in captivity.[111] This situation and others will require a court to consider whether, in addition to domestic and bilateral treaty laws, any international conventions implicate Gülen in such a way as to override the political offense exception based on terror-related charges.

C. Crimes Against the Head of State

Finally, careful consideration should be assigned to the charge levied against Gülen regarding conspiracy to assassinate Turkish President Erdogan. Indeed, Turkish fighter jets controlled by pro-coup members of the Turkish military dropped bombs near the presidential palace, and pro-coup soldiers allegedly attempted to abduct the President from his hotel room.[112] Assuming there exists sufficient evidence implicating Gülen in ordering these assaults, the cleric could very well be at risk of extradition under this charge.

---

[108] *Id.*
[109] *Id.*; *see also* Budak, *supra* note 9.
[110] *Turkey's Chief of Staff Hulusi Akbar Rescued from pro-coup Soldiers*, DAILY SABAH (July 16, 2016), https://www.dailysabah.com/politics/2016/07/16/turkeys-chief-of-staff-hulusi-akar-rescued-from-pro-coup-soldiers.
[111] Patrick Kingsley, *Mysteries, and a Crackdown, Persist a Year After a Failed Coup in Turkey*, N.Y. TIMES (July 13, 2017), https://www.nytimes.com/2017/07/13/world/europe/turkey-erdogan-failed-coup-mystery.html.
[112] Will Worley & Chris Stevenson, *Turkey Coup: President Erdogan Purges Military Insurgents After Failed Rebellion as Thousands on Streets in Support*, INDEPENDENT (July 16, 2016), https://www.independent.co.uk/news/world/Europe/turkey-coup-erdogan-latest-news-purge-crackdown-gulen-a7141006.html.

As opposed to the previously discussed allegations against Gülen, crimes against a head of State are expressly barred from protection under the political offense exception by the U.S.-Turkey extradition treaty; article 3 states that any offense committed or attempted against a head of State or a head of government or against a member of their families shall not be deemed an offense of a political character.[113] Thus, any evidence that Gülen conspired to have coup participants assassinate, kidnap, or take hostage Erdogan would unquestionably warrant extradition.

Without clear evidence demonstrating Gülen commanded an offense against Erdogan, the analysis will become more complicated. Although bombs fell near the presidential palace in Ankara, they did not directly strike it.[114] Additionally, Erdogan was not present in the facility during the strike.[115] However, the hotel in which he was staying on the night of the coup was raided—the President being tipped-off and fleeing shortly beforehand.[116] Turkish authorities contend this was a kidnapping attempt executed by rogue Turkish military commandos. [117] A court analyzing this scenario will inevitably be forced to make a determination based on the facts provided as to whether an act or an attempted act against President Erdogan was committed and whether probable cause exists linking Gülen to the act(s). If such evidence exists, this charge would likely provide grounds for Gülen's extradition.

CONCLUSION

In examining the political offense exception and Turkey's extradition request for Fethullah Gülen, it becomes clear that a lack

[113] *See* Treaty on Extradition and Mutual Assistance, Turkey-U.S., art. 3, § 1(a), June 7, 1979, 3 U.S.T. 3111.
[114] *See* Worley & Stevenson, *supra* note 112.
[115] *Id.*
[116] Constanze Letsch & Philip Oltermann, *Turkey Arrests 1 soldiers Over Alleged Erdogan Kidnap Bid*, GUARDIAN (Aug. 1, 2016), https://www.theguardian.com/world/2016/aug/01/turkey-arrests-11-soldiers-over-alleged-erdogan-kidnap-bid.
[117] *Id*.

of sufficient evidence is not Turkey's only barrier to extraditing the alleged coup mastermind. Should sufficient evidence of Gülen's crimes be provided to the Department of State, Turkey will continue to wage an uphill battle in its quest to extradite the U.S.-based cleric due to the nature of the political offense exception as applied by U.S. federal courts. In addition to proving that probable cause exists linking Gülen to the alleged crimes, Turkey must demonstrate that such crimes are neither a pure nor relative political offense. This political offense determination would prove a challenge not only for Turkey, but for the Court conducting the probable cause hearing. While pure political offenses are determinable based on relatively clear-cut and universally recognized principles, relative political offenses will require the court to apply one of several competing theories to its analysis—immediately opening the process to allegations of subjectivity and bias. Nevertheless, such is the present state of the political offense exception as applied in the United States.

SECURING THE CENSUS: ASSESSING THE CYBERSECURITY OF THE 2020 CENSUS IN AN AGE OF INFORMATION WARFARE

By: Garrett Mulrain[*]

INTRODUCTION

Census 2020 will be the first in U.S. history to use the internet to undertake the monumental challenge of counting every single person in the country. The use of web-based tools and modern equipment will undoubtedly lead to increases in efficiency for those counted, as well as for the Census Bureau itself. However, with new technological innovation comes new cybersecurity challenges, and the challenges threatening Census 2020 are nothing short of existential for the United States. As it stands, there is less than a year before this process officially begins, and by all accounts, the United States is not prepared.

This essay will be divided into four sections. First, the Article will detail a brief overview of the census. Second, it will

[*] Garrett Mulrain is a licensed attorney and is currently working as Associate Counsel for a federal agency. He was previously awarded a clerkship with the American Bar Association Standing Committee on Law & National Security, and oversaw a portfolio that included cyberwarfare, national security law, the intelligence community, privacy litigation, the Military Commissions at Guantanamo Bay, and National Defense Authorization Acts. Prior to that clerkship, Mr. Mulrain worked with the Civil Rights Division of the Department of Homeland Security's Transportation Security Administration. He has previously worked with the International Criminal Tribunal for the Former Yugoslavia in the Hague, Human Rights Watch before the European Parliament in Belgium, and as a clerk for the Egyptian-American Rule of Law Association. Mr. Mulrain earned an LL.M. in National Security & U.S. Foreign Relations Law, with highest honors, from the George Washington University Law School, and an LL.B. from University College Cork, Ireland. The views and opinion expressed in this article are those of the author and do not necessarily reflect the official policy or position of any agency of the U.S. Government.

contextualize the information-warfare era in which we live. Next, this Article will assess the current state of cybersecurity of Census 2020 by detailing security concerns that have already been identified. Finally, methods for reform will be suggested in the hope that their implementation now could help stem the threat towards Census 2020.

I. BACKGROUND

A. What Is It? An Overview of the Census

Article I of the U.S. Constitution states that "Representatives and direct taxes shall be apportioned among the several States … according to their respective numbers . . . ."[1] This is often read in conjunction with a later section, detailing that "[n]o capitation, or other direct, tax shall be laid, unless in proportion to the census or enumeration herein before directed to be taken."[2] From this authority, a national census of the "actual enumeration" of the population is taken every ten years.[3] The census also has an extensive history of legislative reform.[4]

---

[1] U.S. CONST. art I, § 2, cl. 3.

[2] U.S. CONST. art I, § 9, cl. 4. These articles have also been bolstered by the 14th Amendment, which is outside the scope of this article. U.S. CONST. amend. XIV.

[3] Nathaniel Persily, *The Law of the Census: How to Count, What to Count, Whom to Count, and Where to Count Them*, 32 CARDOZO L. REV. 755, 758 (2011).

[4] While the Constitution is the cornerstone of Census 2020's authority, that authority has been repeatedly strengthened and reformed by subsequent legislation. To just name a few pieces of legislation, the Census Bureau became a permanent agency from an act passed in 1902. An Act to Provide for a Permanent Census Office, ch. 139, 52 Stat. 51 (1902) (current version at 13 U.S.C. § 3 (2012)). The Reapportionment Act of 1929 authorized the corresponding reapportionment of seats for the House of Representatives, and for the first time, made that reapportionment automatic for each subsequent census. Reapportionment Act of 1929, ch. 28, 46 Stat. 21 (1929) (current version at 2 U.S.C. § 2(a) (2012). Legislation in 1954 collected and codified under the laws of the Census under Title 13 of the U.S. Code, where they are

Among many other key uses, the Census controls the apportionment of seats allotted in the House of Representatives[5] and its data is also used to distribute as much as $675 billion of federal funding.[6] Census data is used to decide the location of housing programs and public facilities, plan national transportation systems across the United States, examine demographic changes to reassess policy and legislative impacts, and is the backbone for a host of other topics.[7] As such, the census is often a hot political topic. Debates embroil the sphere of *who* to count, and have included overseas troops, college students,[8] incarcerated individuals,[9] and non-citizens.[10] Debates have also focused on *how* to count, as different

---

still found today. And more recently, the *Confidential Information Protection and Statistical Efficiency Act of 2002*, "[e]nhance[d] the management and promotion of electronic government services and processes by establishing a federal Chief Information Officer within the Office of Management and budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to government information and services, and for other purposes." Confidential Information Protection and Statistical Efficiency Act of 2002, Pub. L No. 107-347, 116 Stat. 2899 (2002); *see, e.g.*, *Legislation 1989 - Present*, U.S. CENSUS BUREAU, https://www.census.gov/history/www/reference/legislation/legislation_1989_-_present.html (last visited May 22, 2019).

[5] U.S. CONST. art I, § 2.

[6] Numbers taken from a recent Census Bureau estimate from 2015. *See also* MARISA HOTCHKISS & JESSICA PHELAN, USES OF CENSUS BUREAU DATA IN FEDERAL FUNDS DISTRIBUTION, U.S. CENSUS BUREAU (Sept. 2017), https://www.census.gov/library/working-papers/2017/decennial/census-data-federal-funds.html.

[7] *See* Nick Hart & Meron Yohannes, *Why an Accurate Census Count in 2020 Matters*, BIPARTISAN POLICY CTR. (Nov. 21, 2018), https://bipartisanpolicy.org/blog/why-an-accurate-census-count-in-2020-matters/.

[8] *The Census: College Students Count - but Where?*, PEW CHARITABLE TRUST (Mar. 16 2010), https://www.pewtrusts.org/en/research-and-analysis/reports/2010/03/16/the-census-college-students-countbut-where.

[9] *U.S. Census and Incarceration*, BRENNAN CTR. FOR JUSTICE (Jan. 27, 2010), https://www.brennancenter.org/analysis/us-census-and-incarceration.

[10] Edith Honan & Tara Bahrampour, *Trial Over Census Citizenship Question Closes with Arguments Over Government's Motives*, WASH. POST (Nov. 27, 2018), https://www.washingtonpost.com/local/social-issues/trial-over-citizenship-question-closes-with-arguments-over-governments-motives/2018/11/

methods such as sampling or imputing census results have often tipped the balance of House seats or federal funding.[11] There are also direct security implications, as "state and local police departments also use census data for crime mapping and forecasting to determine the effective allocation of law enforcement resources."[12] State and local governments, as well as research centers and policy organizations, all rely on this information to assess the current functionality of government programs.

Despite being the subject of public debate every decade, the United States is not doing all it can to protect Census 2020 from the cybersecurity threats that our nation will face. Perhaps even worse, since census data is so vital to our everyday lives, if that data is lost, hacked, or altered, the full extent of the damage is potentially unknowable.

B. Why Does This Matter? The Cybersecurity Concerns

At the simplest level, Census 2020 is charged with collecting information. As noted, the data collected is vitally important for the various functions of the society of the United States. Perhaps more than from any other source, data collected from the 2020 Census will be relied upon for the next decade. All of this data is aggregated, dissected, and analyzed for many purposes, and thus is some of the most important data available. As a new feature, Census 2020 will be implemented with, and rely on, the internet. This comes at a time however, when information and the internet are being utilized as weapons of war.

27/90e1b01e-f28c-11e8-aeea-b85fd44449f5story.html?utm_term=.93286469 2f bd.

[11] *See* Persily, *supra* note 3.

[12] *An Accurate Census is Essential for a Strong America*, COUNCIL FOR A STRONG AMERICA (Nov 9, 2017), https://www.strongnation.org/articles/515-an-accurate-census-is-essential-for-a-strong-america.

1. Information warfare

The use and abuse of information has become a theme in the 21st century, and the impact on U.S. security appears in headlines almost daily. While Russian hackers work round-the-clock to gather *kompromat* on foreign governments,[13] North Korea and other autocratic rulers manipulate information to keep their own citizens in the dark.[14] Information warfare impacts the global economy, for example, when China engages in large-scale intellectual property theft.[15] In March 2017, Wikileaks published classified information on software tools used by the Central Intelligence Agency–exposing national security methods used to protect the United States.[16] Reports found that Russians involved in the meddling of the 2016 election "were successful in stealing the personal information from as many as 500,000 voters from one state's board of

[13] Greg Myre, *A Russian Word Americans Need to Know: 'Kompromat,'* NPR (Jan. 11, 2017), https://www.npr.org/sections/parallels/2017/01/11/509305088/a-russian-word-americans-need-to-know-kompromat.

[14] For example, the famed "great firewall of China" uses various internet-based tools to filter what information is censored when running through Chinese networks. Foreign websites and sites critical of the Chinese government are often blocked. *See* Chris Hoffman, *How the "Great Firewall of China" Works to Censor China's Internet*, HOW-TO-GEEK (Sept. 10, 2017), https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/.

[15] Examples of Chinese intellectual property theft are so common that the Department of Justice ("DOJ") actually has initiatives aimed at tackling this "economic espionage" specifically from China. No other country has been given this extent of DOJ attention when it comes to the protection of U.S. trade secrets. *See recently* Jeff Sessions, Attorney General, Dept. Of Justice, Remarks as Prepared for Delivery in Washington, D.C.: New Initiative to Combat Chinese Economic Espionage (Nov. 1, 2018), https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage.

[16] Scott Shane, Matthew Rosenberg & Andrew Lehren, *WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents*, N.Y. TIMES (Mar. 7, 2017), https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html.

elections website."[17] These efforts are being waged primarily through cyber means, and as risks associated with new technologies becomes clearer, there are no signs of information warfare slowing down.

Specific hacks have also proven that there is an inherent value in targeting large databases, as they are often a trove of personally-identifiable information (PII). In 2015, the U.S. Office of Personnel Management (OPM) was specifically targeted because it housed some of the U.S. Government's most personal information, and it is estimated that over 20 million records were stolen.[18] A breach at the Yahoo! corporation in 2013 compromised the PII of roughly 3 billion accounts (something that was not fully realized until October 2017).[19] And those examples pale in comparison to the devastation of the 2017 Equifax hack, which resulted in the loss of everything from names to social security numbers for nearly half of the U.S. population.[20] Each of those hacks shared a common theme: a massive database of stored PII, much like what will be assembled

---

[17] *See* Abby Vesoulis, *Why These Former Cybersecurity Officials are Worried About the Census*, TIME (July 19, 2018), http://time.com/5341881/2020-census-cybersecurity-concerns/. As a further example, up to 126 million people saw freely-posted content on social media sites, operated by at least 470 accounts linked to Russia, or affiliated with the Russian Internet Research Agency. *Hearing on Social Media Influence in the 2016 United States Elections: Hearing Before the S. Select Comm. On Intelligence*, 115th Cong. (2017). Up to 10 million Americans are estimated to have viewed an ad that was paid for by Russian accounts. For further information, *see* SUZANNE E. SPAULDING ET AL., CTR. FOR STRATEGIC & INT'L STUDIES, COUNTERING ADVERSARY THREATS TO DEMOCRATIC INSTITUTIONS (Feb. 14, 2018), https://www.csis.org/analysis/countering-adversary-threats-democratic-institutions.

[18] Alan Wehbé, *OPM Data Breach Case Study: Mitigating Personnel Cybersecurity Risk*, 26 B.U. PUB. INT'L L. J. 75, 93 (2017).

[19] Matt O'Brien, *Yahoo: 3 Billion Accounts Breached in 2013. Yes, 3 Billion*, AP NEWS (Oct. 3, 2017), https://www.apnews.com/06a555ad1c19486ea49f6b5b80206847.

[20] *See* Garrett Mulrain and McKay Smith, *Equi-failure: The National Security Implications of the Equifax Hack and a Critical Proposal for Reform*, 9 J. NAT'L SEC. L. & POL'Y 549 (2018).

by Census 2020. In fact, the data contained in Census 2020 is going to be, perhaps, the greatest vault of personal information on U.S. persons ever assembled.

2. Public trust is essential for democracies

Information and public trust are essential components to the democratic functioning of the United States. Simply put, democracies are only possible because the public has confidence in the processes of democracy itself. This includes the election system, trust in law enforcement, rulings from Article III judges, and of course, decennial census results.

Information warfare and public trust also impact different political systems in different ways, particularly democracies versus authoritarian regimes.[21] While disinformation campaigns can act as stabilizing influences for authoritarian regimes, those same forces destabilize the United States.[22] Experts on the impact of misinformation have noted that

> [D]emocracies, are vulnerable to information attacks that turn common political knowledge into contested political knowledge. If people disagree on the results of an election, or whether a census process is accurate, then democracy suffers. Similarly, if people lose any sense of what the other perspectives in society are, who is real and who is not real, then the debate and argument that democracy thrives on will be degraded.[23]

---

[21] HENRY FARRELL & BRUCE SCHNEIER, BERKMAN KLEIN CTR., RESEARCH PUB. NO. 2018-7, COMMON KNOWLEDGE ATTACKS ON DEMOCRACY (Oct. 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273111.
[22] Henry Farrell & Bruce Schneier, *Information Attacks on Democracies*, LAWFARE (Nov. 15, 2018, 10:35 AM), https://www.lawfareblog.com/information-attacks-democracies.
[23] *Id.*

Bolstering public confidence in democratic processes and institutions is paramount for the strength and maintenance of a democracy.[24] This undoubtedly includes increasing public trust in the results of a census, and that comes from ensuring robust cybersecurity protections for Census 2020.

3. Information warfare and public trust: trends and examples

Unfortunately, public confidence in democratic institutions is already showing signs of erosion. While the United States is arguably built upon a certain level of mistrust, recent polling shows that the public's trust in Congress is dwindling to an all-time low.[25] That mistrust has also spread to other portions of U.S. society, such as the federal government and media organizations.[26] When compared with other countries, Edelman, a leading marketing firm, has found that out of twenty-eight different countries surveyed, the United States has had the highest loss of trust in "government, media, business, and NGOs" from 2017 to 2018.[27] When questioned about this trend, a leading Edelman researcher, David Bersoff, noted that "the lifeblood of democracy is a common understanding of the facts and information that we can then use as a basis for negotiation and compromise … when that goes away, the whole foundation of democracy gets shaken."[28]

Recent examples of public mistrust are playing out daily against democratic systems and procedures. In August 2017, a woman from Iowa was charged with attempting to vote twice

---

[24] *Id.*

[25] C.K., *Why America Has a Trust Problem*, ECONOMIST (Apr. 25, 2017), https://www.economist.com/democracy-in-america/2017/04/25/why-america-has-a-trust-problem.

[26] Uri Friedman, *Trust is Collapsing in America*, ATLANTIC (Jan. 21, 2018), https://www.theatlantic.com/international/archive/2018/01/trust-trump-america-world/550964/.

[27] *Id.; 2019 Edelman Trust Barometer*, EDELMAN, https://www.edelman.com/trust-barometer (last visited May 23, 2019).

[28] Friedman, s*upra* note 26.

because she believed that "the election was rigged and her first ballot would be changed."[29] Article III judges, who are entrusted to uphold the law, are increasingly tarnished, as evidenced most clearly by public lambasting in February 2018 of the Foreign Intelligence Surveillance Court (FISC) judges.[30] Trends and examples also show that mistrust in democracies is not isolated–it can even lead to support for more populist and authoritarian political candidates.[31] So, in an age of public mistrust, where databases are targeted systematically by foreign adversaries, it must be asked: does Census 2020 have strong cybersecurity protections?

C. How Prepared Are We? The Current State of Census 2020

1. The Census Bureau's posture and the Georgetown Letter

As mentioned earlier, with Census 2020 being the first to completely adopt the internet, threats facing Census 2020 are more

[29] Maya Oppenheim, *Iowa Woman Who Tried to Vote for Donald Trump Twice Gets Two Years Probation and $750 Fine*, INDEPENDENT (Aug. 18, 2017), https://www.independent.co.uk/news/world/americas/terri-lynn-rote-iowa-vote-donald-trump-twice-two-years-probation-750-fine-a7900886.html.

[30] While the purpose of this Article is not to examine calls for more transparency from the FISC, the fact that the Court and the judges who sit on it were criticized over social media demonstrates an example of erosion towards the judicial institution as a whole. *See* Louise Matsakis, *Reading Between the Lines of the Devin Nunes Memo*, WIRED (Feb. 2, 2018), https://www.wired.com/story/devin-nunes-memo-carter-page-surveillance/; *see also* Aaron Mackey, *New Surveillance Court Orders Show that Even Judges Have Difficulty Understanding and Limiting Government Spying*, ELEC. FRONTIER FOUND. (Sept. 11, 2018), https://www.eff.org/deeplinks/2018/09/new-surveillance-court-orders-show-even-judges-have-difficulty-understanding-and.

[31] Neil Howe, *Are Millennials Giving Up on Democracy?*, FORBES (Oct. 31, 2017), https://www.forbes.com/sites/neilhowe/2017/10/31/are-millennials-giving-up-on-democracy/#48b56d292be1; *see also* Mark Triffitt, *A Growing Mistrust in Democracy is Causing Extremism and Strongman Politics to Flourish*, THE CONVERSATION (July 9, 2018), https://theconversation.com/a-growing-mistrust-in-democracy-is-causing-extremism-and-strongman-politics-to-flourish-98621.

prevalent than ever.[32] In a National Advisory Committee Meeting in the spring of 2018, Kevin Smith, the Census Bureau Associate Director for Information Technology and Chief Information Officer, was forthcoming about the *Continually Evolving Cybersecurity Program for the 2020 Census.*[33] Kevin Smith noted in his presentation that "cybersecurity is our highest IT priority,"[34] and listed key components to the Census Bureau's strategy, including public perception and trust, addressing cyber threats, an effective design, and the Census Bureau's approach itself.[35] From the Census Bureau's perspective, the priorities of data security and user experience are actually mutually exclusive; the more that the user-experience rises, the more it takes away from data security.[36] The Census Bureau's risk strategy focuses on mitigating internal security threats, such as faulty employee devices and insider threats. It also includes strategic partnerships for addressing external threats, such as breaches from internet providers and foreign phishing sites.[37] The Census Bureau relies on the NIST cybersecurity framework, which rightfully should be the industry standard.[38]

---

[32] *See* Jory Heckman, *Census Bureau Runs Drills with DHS to 'Stay Ahead of Cyber Threats'*, FED. NEWS NETWORK (Oct. 19, 2018), https://federalnewsnetwork.com/cybersecurity/2018/10/census-bureau-runs-drills-with-dhs-to-stay-ahead-of-cyber-threats/ (noting that "Simson Garfinkle, a senior computer scientist for confidentiality and data access at the Census, said advances in computer power in the last decade have made it easier to unscramble the aggregated data the agency releases to the public," and that this unscrambling of data makes the risk of hacking a Census database particularly relevant, as unscrambled data would directly expose the personally identifiable information of potentially millions of U.S. citizens).

[33] KEVIN SMITH, U.S. CENSUS BUREAU, CONTINUALLY EVOLVING CYBERSECURITY PROGRAM FOR THE 2020 CENSUS, NATIONAL ADVISORY COMMITTEE SPRING 2018 MEETING (June 14, 2018), https://www2.census.gov/cac/nac/meetings/2018-06/smith-cybersecurity.pdf.

[34] *Id.* at 3.

[35] *Id.* at 4.

[36] *Id.* at 5.

[37] *Id*. at 7.

[38] NAT'L INST. OF STANDARDS AND TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, VERSION 1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (while the

Despite the welcomed language from the Spring 2018 meeting, many industry experts still remain unconvinced. In a letter to Commerce Secretary Wilbur Ross and Acting Director of the Census Bureau Ron Jarmin, top civil servants from various government security offices, wrote that "while the Bureau has released a considerable array of materials regarding the 2020 Census and even aspects of its electronic component, to the best of our knowledge none specifies how the Census Bureau is implementing even the most basic cybersecurity practices."[39] The experts questioned whether or not the Census Bureau is abiding by basic cybersecurity standards, including the implementation of two-factor authentication, encryption of sensitive data in transit and at rest, the specific encryption methods that will be used, and "whether other now-standard cybersecurity practices will be utilized."[40] Importantly, this letter was released after the methods from the Spring 2018 meeting were publicized. The Georgetown Letter is correct; by simply describing the threat, the Census Bureau has only demonstrated that it understands what the threat is. It does not demonstrate that they are currently prepared to face it.

In response to the Georgetown letter, the Census Bureau released a statement defending its cybersecurity programs.[41] The statement reads that the Census Bureau has

---

NIST Cybersecurity Framework is beyond the scope of this article, it is widely regarded as one of the best cybersecurity guides available, and as such, comes highly recommended by government and private-industry experts alike); s*ee also* Paul Rosenzweig, *NIST Cybersecurity Framework Issued*, LAWFARE (Feb. 12, 2014), https://www.lawfareblog.com/nist-cybersecurity-framework-issued.

[39] Letter from the Institute for Constitutional Advocacy and Protection et al., Georgetown University Law Center (July 16, 2018) [hereinafter Georgetown Letter], https://www.law.georgetown.edu/icap/wp-content/uploads/sites/32/2018/07/Census-Cybersecurity-Letter.pdf.

[40] *Id.* at 1.

[41] Kriston Capps, *Security Experts Warn Census Bureau: Beware of Hackers*, CITYLAB (July 20, 2018), https://www.citylab.com/equity/2018/07/what-if-the-russians-hack-the-census/565379/.

> incorporated industry best practices and follow[s] Federal IT security standards for encrypting data in transmission and at rest. As a matter of data security, we do not disclose our specific encryption methods, but we would like to note, in response to the concerns of the letter, that two-factor authentication is required for all who access the data. While many of our defenses are invisible to the public, know that we have strong and resilient security measures protecting every respondent's information.[42]

That statement can be read in two different ways. On the one hand, the Census Bureau is aware of public trepidation regarding the risk to the information and is implementing a few of the specific cybersecurity norms that are called for (data encryption in transit and at rest, and two factor authentication). The other way to read that statement is as a brief, single paragraph, that goes out of its way to reject a call for transparency. In an attempt to bolster public confidence in its methods after a critical letter was published, the Census Bureau actually forfeited public transparency, and thereby risks eroding public confidence. This would not be a huge problem if the Census Bureau was engaging in best practices; however, recent watchdog reports suggest that the Census Bureau may not actually have the "strong and resilient security measures" that they claim to.[43]

2. The Government Accountability Office report

While there is more than one Government Accountability Office (GAO) report issued on the current preparedness of the 2020

[42] Press Release, U.S. Census Bureau, No. CB18-RTQ.04, Census Bureau's Cybersecurity Posture (July 18, 2018), https://www.census.gov/newsroom/press-releases/2018/cybersecurity.html.
[43] *Id.*

Census,[44] the April 2018 Report stands out.[45] By the numbers, the GAO report found that of the eighty-four recommendations made to the Census Bureau, at the time of the report as many as thirty of those recommendations had not been fully implemented.[46] Despite being added to GAO's "high-risk list" in February 2017, the Census Bureau's inability to implement some of those recommendations in a timely fashion "is more critical than ever."[47] Couple those inefficiencies with the lack of transparency that the Census Bureau boasts about,[48] and potential cybersecurity threats become a very real possibility. Among other recommendations, the GAO found that the scaling back of testing to new software and capabilities introduced new security challenges to the already-difficult enumeration task.[49] In a troubling statement the GAO remarked that "without sufficient testing, operational problems can go undiscovered and the opportunity to improve operations will be lost."[50]

In addition to field testing and software security issues, the GAO report made two other findings. First, the inability to effectively implement testing procedures actually comes from

---

[44] *See Information Technology: Uncertainty Remains About the Bureau's Readiness for a Key Decennial Census Test*: *Testimony Before the Subcomm. on Gov't Operations, H. Comm. on Oversight and Gov't Reform*, 114th Cong. (2016) (statement of David A. Powner, Gov't Accountability Office, Dir. Info. Tech. Mgmt. Issues) [hereinafter Powner Testimony], https://www.gao.gov/assets/690/681079.pdf.

[45] *2020 Census: Continued Management Attention Needed to Mitigate Key Risks Jeopardizing a Cost-Effective and Secure Enumeration: Testimony Before the Subcomm. on Commerce, Justice, Sci., and Related Agencies H. Comm. on Appropriations*, 115th Cong. (2018) (statements of Robert Goldenkoff, Dir., Strategic Issues, Gov't Accountability Office, and David A. Powner, Dir., Info. Tech., Gov't Accountability Office), https://www.gao.gov/assets/700/691316.pdf.

[46] *Id.* at 1.

[47] *Id.*

[48] Press Release, U.S. Census Bureau, *supra* note 42.

[49] *Id.*

[50] *Id.*

mismanagement and flaws in Census Bureau oversight.[51] A new director was recently appointed to the Census Bureau,[52] however that new management team will have their hands full with such a small window to correct the existing inefficiencies. Second, the GAO report found that inaccurate cost estimation from the Census Bureau impacts their overall effectiveness.[53] Census 2020 is undoubtedly one of the most expensive ever, and an agency that cannot adequately estimate their own budget risks not knowing how to effectively operate within that budget.

Therefore, recommendations are not yet implemented, software testing is being scaled back, and management is not conducting oversight while operating with an inaccurate budgeting process. Couple this with an ever-dwindling time frame, and Census 2020 seems less like it will be prone to threats, and more of an outright recipe for cyber failure.

3. The Inspector General report

The multiple findings of the GAO are not the only recent report that is critical of the cybersecurity posture of Census 2020. The Department of Commerce's own Office of the Inspector General (OIG) issued a warning to the Census Bureau as recent as October 2018.[54] And even though the OIG report found that the Census Bureau was receptive to their recommendations, it is alarming that the following critical security flaws are still inadequate this close to 2020.

---

[51] *Id.*

[52] Hansi Lo Wang, *Senate Confirms Trump's Census Bureau Director Nominee Steven Dillingham*, NPR (Jan. 2, 2019), https://www.npr.org/2019/01/02/667063727/senate-confirms-trumps-census-bureau-director-nominee-steven-dillingham.

[53] Powner Testimony, *supra* note 45, at 7.

[54] U.S. DEP'T OF COMMERCE, OFFICE OF INSPECTOR GEN., THE CENSUS BUREAU MUST IMPROVE ITS IMPLEMENTATION OF THE RISK MANAGEMENT FRAMEWORK, OIG-19-002-A (Oct 30, 2018), https://www.oversight.gov/sites/default/files/oig-reports/2018-10-30_Census%20RMF_Final%20Audit%20Report.pdf.

First, the OIG report found that the "Bureau had not continuously monitored critical security controls and failed to document the resulting risks."[55] Those controls and monitoring are the process that the Census Bureau has in place for continuously reassessing their individual cybersecurity systems. OIG examined various systems related to internal controls and security maintenance and found that almost *half* of internal monitoring controls had not been assessed within the recommended time frame.[56] In fact, some of the "highest risk controls" had not been assessed since 2012.[57] Even worse, when this failure was highlighted to the Census Bureau's Chief Information Officer and Chief Information Security Officer, they stated that "they were unaware that the periodic assessments were not occurring."[58]

That startling realization was also a theme of the OIG report for its second conclusion: "authorizing officials lacked information about significant cybersecurity risks."[59] The Census Bureau has software designed to automate its own unique framework for internal monitoring called the Risk Management Program System ("RMPS"). According to OIG, when these RMPS reports are wrong or inadequate, it causes management to not have an accurate portrayal of their current cybersecurity risks.[60] In essence, while the management knew which cybersecurity controls were important, they were unaware of the functionality of those systems, as well as how they were actually implemented.[61] This would lead anyone to question the previous statements from Census Bureau officials to Congress and the media prior to this OIG report: if officers were unaware of their own internal cybersecurity failures, how could they give an accurate assessment in media statements or to lawmakers?[62]

---

[55] *Id.* at 2.
[56] *Id.* at 3.
[57] *Id.*
[58] *Id.*
[59] *Id.* at 4.
[60] *Id.*
[61] *Id.* at 5.
[62] Specifically, that inaccurate information is highlighted in the OIG report as well. As many as one-third of security control assessments did not have valid

Finally, the OIG report found that the broader system of common controls was ineffective for the systems they monitor. A common control is a widespread system that is charged with monitoring and effectively implementing multiple systems, i.e. individual systems share one common control center.[63] The OIG report found that the smaller systems did not "inherit" the common control correctly.[64] This inheriting flaw demonstrates that, not only are the individual systems inaccurate, the overall common control system that works to keep them accurate, was also flawed.[65]

When reading the OIG report in tandem with the GAO report, the outlook is not only bleak–it represents a serious cybersecurity concern. Internal security controls are flawed, and their common control method is inaccurate. That inaccuracy is not always adequately monitored, and Census Bureau management may be ignorant to those faults. Finally, in public statements and Congressional testimony, Census Bureau officials paint a reassuring picture of their ability to be secure for Census 2020. That outlook is not warranted,[66] and since these security fixes are pressed for time while operating in an age of information warfare, robust reform is needed now.

II. WHAT CAN WE DO? SUGGESTIONS FOR REFORM

As noted, the crux of this paper is to raise awareness of the risks facing Census 2020 and to put that into the context of this era of information warfare and public mistrust. While this list is far from

---

documentation. Furthermore, systemic date inconsistencies in the RMPS reports had reduced the credibility of those reports themselves. And finally, the RMPS risk scores "were not reflective of actual risk." *Id.* at 5-7.

[63] *Id.* at 8.

[64] *Id.*

[65] *Id.* at 8-9.

[66] *See* Aaron Boyd, *Census Bureau Isn't Properly Managing its Risk Management Review System*, NEXTGOV (Nov. 2, 2018), https://www.nextgov.com/cybersecurity/2018/11/census-bureau-isnt-properly-managing-its-risk-management-review-system/152530/.

complete, there are some broad reforms that can be implemented to mitigate the current threat landscape.

A. Implement Suggestions from the Georgetown Letter, GAO Reports, and OIG Reports

The first suggestion for reform is also the most straightforward: the Census Bureau should take and implement those considerations already laid out before them. These fixes vary widely in complexity, and while they hopefully will be introduced by the time of this writing, taking stock of the suggestions made by industry leaders and government agencies can only help ensure better security for Census 2020.

In particular, the Census Bureau should implement those basic cybersecurity practices. This includes two-factor authentication, the encryption of sensitive data both in transit and at rest, using modern and effective encryption methods, and following other "now-standard cybersecurity practices."[67] Those standard cybersecurity practices should reflect the most up-to-date NIST standards, as they are widely regarded as representing the industry best practice.[68]

From the GAO report, the Census Bureau should work to implement the roughly thirty recommendations that had not yet been fully realized. The Census Bureau should ramp-up testing of operational programs to ensure that they are fully ready for enumeration day. Even if this is not totally feasible, the testing should be prioritized so that the software and counting implementation is as technologically secure as possible. Finally, the Census Bureau should prioritize streamlining its management oversight and consider contracting outside firms or agencies to conduct financial audits. This will allow the Census Bureau to better estimate

[67] Georgetown Letter, *supra* note 39, at 1.
[68] NIST, *supra* note 38.

its resources and needs, thereby ensuring a smooth census process.

And finally, from the OIG report, the Census Bureau should continuously monitor its critical security controls and the common controls that oversee them. It should ensure correct audit reporting going forward, so as to gain the most up-to-date information from the RMPS reports. Finally, the officers and managers of the Census Bureau need to be better versed on how the earlier reports were wrong and how the controls were untested or broken. That increase in knowledge should be applied through all management of the agency to ensure that gaps in knowledge are not unwittingly passed along to Congress, the media, or other agencies.

B. Change the Perception Towards Transparency

To be sure, it is entirely possible that the Census Bureau will be able to fix all of their cybersecurity systems in time and that Census 2020 goes forward without so much as a successful phishing email. And while that would be the optimal outcome, the Census Bureau also needs to appreciate that we are living in the age of information warfare. The authenticity of census population counts can be called into question, even if those results are completely accurate. For that reason, the Census Bureau should prioritize establishing more trust with the public. Public trust in a democratic system comes largely through transparency. That transparency could come in many forms. The Census Bureau could publish biweekly or monthly reports about the cybersecurity fixes it is implementing, with detailed assessments for the technology sector, as well as a general version for the wider public. The Census Bureau might consider more audit requests, which could then be publicized. Taking some advice from the Georgetown Letter, the Census Bureau could consider partnering with a number of private cybersecurity consulting firms to get an independent, non-government perspective.

C. Congress Should Use its Oversight Authority

As in any democracy, the ultimate blame for a potentially-flawed cybersecurity posture could and should rest with our elected leaders. The Census Bureau has not always proved fully willing to work with congressional leaders.[69] Given the fact that there remains less than a year to bolster the cybersecurity of the Census, Congress should not feel trepidation about using its oversight authority.

If the Congressional requests for information remain unanswered, and Congress feels it is truly warranted, then a limited investigation or a subpoena for testimony could prove fruitful. Granted, this should be used as a last resort, but time is of the essence, and the Census Bureau has given no indication of becoming a more transparent agency. Again, if the Census Bureau's database of PII is hacked and information on hundreds of millions of Americans is compromised, then Congress should shoulder some of the blame.

D. Building Intergovernmental Cooperation

Finally, the Census Bureau should continue to build on the robust partnerships that it has claimed.[70] The Census Bureau should make use of the intelligence community, as well as other federal

---

[69] *See* Salvador Rizzo, *Wilbur Ross's False Claim to Congress That The Census Citizenship Question Was DOJ's Idea*, WASH. POST (July 30, 2018), https://www.washingtonpost.com/news/fact-checker/wp/2018/07/30/wilbur-rosss-false-claim-to-congress-that-the-census-citizenship-question-was-dojs-idea/?utm_term=.07e596f887af (claiming that Commerce Secretary Wilbur Ross has attempted to bypass Congressional queries about whether or not the Department of Commerce originally planned on putting a question regarding citizenship on Census 2020); *see also Congress Questions Commerce, Census on Citizenship Question*, CONSORTIUM OF SOC. SCI. ASS'N (May 15, 2018), https://www.cossa.org/2018/05/15/congress-questions-commerce-census-on-citizenship-question/.

[70] Phil Goldstein, *Census Bureau to Tap Other Agencies for Cybersecurity Help*,

agencies to best implement a secure census. This could include the National Security Agency, the Federal Bureau of Investigation, and the Department of Homeland Security.[71] The White House could consider an Executive Order to streamline this cooperation, as this process is clearly within the national security realm and would be limited to technological protection of the Census Bureau's databases. This Executive Order could also sunset after that data is fully collected, aggregated, scrambled, and ultimately destroyed. This would ensure maximum protection at all phases of the Census Bureau's work.

CONCLUSION

This Article was not a blind attempt to take away from the tireless work of the Census Bureau and its employees. Every ten years it seems that the agency is thrust into the spotlight with another controversy, and yet it is entrusted with one of the most vital, and perhaps, most under-appreciated constitutional duties. This article was simply an effort to lay out what the census is, why it matters, how prepared we are, and what we as a nation can do to ensure adequate protections for our PII and ultimately, our democratic institutions.

This is an age where information is being weaponized and where public trust in democratic institutions is repeatedly under attack. To many, the census process may be simply counting people and nothing more than that. But if that information is stolen, altered, released, or corrupted, the ripple effects across the United States are potentially unknowable. There is less than a year left to get this right, and as of this writing, the United States is not prepared.

FED. TECH. MAGAZINE (Aug. 15, 2018), https://fedtechmagazine.com/article/2018/08/census-bureau-tap-other-agencies-cybersecurity-help.

[71] *See id*.; *see also* Heckman, *supra* note 32.