2020 Cybercrime Economic Costs: No measure No solution

Jart Armin, Bryn Thompson
CyberDefcon.com/HostExploit.com
CyberROAD Project
jart@cyberroad.eu

Piotr Kijewski
CERT. Polska/NASK
CyberROAD Project
piotr.kijewski@cert.pl

Davide Ariu, Giorgio Giacinto, Fabio Roli
UNICA
CyberROAD Project
giacinto@diee.unica.it

***Abstract*— Governments needs reliable data on crime in order to both devise adequate policies, and allocate the correct revenues so that the measures are cost-effective, i.e., the money spent in prevention, detection, and handling of security incidents is balanced with a decrease in losses from offences. The analysis of the actual scenario of government actions in cyber security shows that the availability of multiple contrasting figures on the impact of cyber-attacks is holding back the adoption of policies for cyber space as their cost-effectiveness cannot be clearly assessed. The most relevant literature on the topic is reviewed to highlight the research gaps and to determine the related future research issues that need addressing to provide a solid ground for future legislative and regulatory actions at national and international levels.**

Keywords*— *Cybercrime, quantifiable, economic costs, measurement, methodology, 2020, security, cyber security, National Security, cyber threats, research gap, CyberROAD, DDOS, botnet trust, taxonomy, metrics, standards, benchmarking, data, definitions, government, governance, policy, budget, insurance, financial, social, impact, ENISA, EWI,

I. INTRODUCTION

In a response to the 2015 CyberROAD survey question to stakeholders: "Have you experienced a cybercriminal action in the last 5 years?" 78% of the respondents responded they had, either in a personal capacity (31%) or through work (47%). When asked "To make the Internet a safer place and to fight cybercrime, what are the topics we should research into?", most respondents rated "Better metrics and statistics on cybercrime" as their 2nd choice (from 6) in order of importance.[1].

Cybercrime has climbed to the top tier in the National Security Strategy of many EU states e.g. France, the Netherlands and the UK, becoming the #1 threat above organized crime and fraud generally. However as indicated within a recent 2013 study for the European Parliament - Directorate General for Internal Policies "The Economic, Financial & Social Impacts of Organized Crime in the EU", "estimates of cybercrime costs are highly contested". It concludes by saying "So is cybercrime a threat, and to whom? It is a threat to all of us. The question is how much of a threat, and how can we better understand how much of a threat it is." [1]

Using property crime, for example, as a comparison, in most countries the metrics are mostly readily available. In the US, the FBI's Uniform Crime Report details how many offenses were committed nationally in 2011 (9,063,173) and of what type (burglary 24%, larceny 68% and motor vehicle theft 7.9%). It is not too difficult from this point on to provide an accurate estimate of the cost of overall property crime to the US economy in 2011 (€14bn). "However, when enquiring about the direct costs of cybercrime to any economy, individual industries, or companies and you get no straight answers." [2]

Worryingly, our awareness of the extent of the problem has advanced very little over the years. At the turn of the millennium cybercrime was recognised as "the organized crime of the 21st century." [3] An article published in Bloomberg Business in 2006, announced that in the previous year, for the first time, "proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, according to an adviser to the U.S. Treasury Dept." [4]. In truth, we are no closer now in knowing how accurate an assessment that was, despite the vast sums spent in the meanwhile. The 2006 Bloomberg article and the problems it summarises could have been written today.

Certainly, there is no lack of reporting on the cost of cybercrime; these make the headlines on a regular basis. But how well do these stand up on closer inspection? Without fundamentally accurate data, how do we know where the research money should be spent? How can policy makers plan for the future? How can boards budget correctly? How can risk be evaluated when data is patchy and unverifiable?

As part of the CyberROAD project this area was viewed from its core foundations. The project established a perspective of where the state of the art is now and needs to be to meet the challenges of the future.

---

[1] [1] CyberROAD Survey Page, http://cyberroad.eu

II. CYBERROAD PROJECT

A. Overview

The aim of the CyberROAD project is to develop a cybercrime and cyber-terrorism research roadmap. Using the knowledge gained in their own areas of expertise, partners from academia, industry, computer security, and legal enforcement agencies, will provide a thorough picture of the current scenario. Through the depiction of future scenarios the most relevant research gaps will be identified and set against the findings from survey-based analyses of stakeholders needs. These will be mapped out to execute a wide-ranging and comprehensive roadmap of the research areas that are needed in order to face forthcoming threats leading up to 2020.

B. The Basics

To review the current economic state-of-the-art an analysis was made of some of the readily accessible data that is fundamental to a study on cybercrime metrics. A variety of sources provided a surprisingly large amount of information. Taken at face value these yield a set of straightforward figures on some of the most contentious issues in cybercrime. In summary:

1) Costs of Cybercrime

* The annual cost to the global economy from cybercrime is more than €300 billion Euros [5]
* Cost of cybercrime for the EU 0.4% of its GDP[2] = €13 billion / annum [6]

Sample EU countries estimates for the cost of cybercrime[3]:

* Poland: € 377 million /annum
* Germany: € 2.6 billion /annum
* UK: € 2 billion /annum

* Cybercriminal revenues (estimate of the cybercrime market itself) €15 billion / annum[4] [7]
* Market for security products and services €50 billion / annum [8]

2) Examples of Cybercrime Metrics

* 3 Billion Users of the Internet (~39% world population) [9]
* Over 200 billion emails processed / day [10]
* 917.9 million Websites (variable) — 39 million / month added (4%) [9]
* IP addresses - IPv4 = 4,294,967,296 (2^{32}) - IPv6 = 128-bits (2^{128}) [11]
* 2.3 billion mobile-cellular subscriptions worldwide [12]
* 1.4 million Browser user agents – bots [13]

3) Technical and Quantitiative Metrics of Cybercrime Activity Indicators

* 85% of processed emails are spam [14]
* 7% of all URLs malicious [15]
* Public Block List count: 1,018,203,532 IP addresses [16]
* 350 million+ in total identifiable malware [17]
* 1 million+ measurable cyber-attacks (variable) [18]
* 330 active Real-time Blackhole Lists (RBL & DNSBL) [19]
* € 7.9 million is the average annualized cost of data breaches [20]
* 10.4% net increase cost of data breaches over the past year [20]
* 250,000 – 500,000 malicious binaries / day [21]
* ~280 million malicious binaries collected [21]
* 6 / 10 million unique IP's sink holed / day [21]
* 900,000 malicious domains / day [21]
* 500 of 52,000 ASNs worldwide (4%) account for hosting 85% of malicious activity [22]

C Overview of Current Estimates

The above examples demonstrate that a variety of data types on cybercrime metrics are available. This is a good starting point. The next step involves evaluating which statistics have value and how they can be used to provide a solid scientific foundation for further study. .

A significant amount of groundwork needs to be covered to attain a practicable framework but the increase in trust derived will effect greater value and improved outcomes. For example, it may be simpler to compute a single 'cost' figure for a whole sector at any one time, which is how cybercrime figures are often portrayed, but unless this stands up to scrutiny the exercise is a complete waste of time and resources. An effective way of working out how, for example, loss of reputation is 'costed' is important as these sums may vary enormously. For instance, a blanket approach may not be accurate enough for budgetary and insurance purposes. The development of a working model is an essential research area if the impact of cybercrime is to be fully understood and appreciated.

III. THE CYBERROAD CYBERCRIME SURVEY

The CyberROAD project designed a broad-based survey in order to gain an understanding of the impact of cybercrime on stakeholders which could be weighed against current research results. It was decided to follow the Delphi approach [5] consisting of an initial poll followed by 2 further questionnaires where participants of the first round are invited to complete at least one, or possibly two, subsequent polls. Answers from the first survey are used to generate more specific questions in the following rounds. A principal area of the CyberROAD surveys centres on 'The cost of cybercrime' in relation to everyday life and business.

1) Purpose

The purpose of the CyberROAD survey is to explore and establish the needs of stakeholders and to find out what they see as the potential threats both now and into the future. As perceived threats may be different from real threats, it is important to try to correlate stakeholders' experiences of cybercrime with the situation as reflected in current reports and analyses. A mismatch between the two can be costly in terms of money spent on research and to stakeholders' understanding of what should or could be done to alleviate risk, i.e., are the right threats being targeted at present?, Can a blanket approach

[2] Estimate of average - range is up to 0.9% of GDP - high-income countries incur higher losses.

[3] Based on share to EU GDP. Figures on GDP are available on the IMF website https://www.imf.org/external/data.htm

[4] CyberDefcon estimate which if only allowing for inflation & not increase is revenues.

[5] http://en.wikipedia.org/wiki/Delphi_method

to security be taken or would a more flexible system be of more benefit?

2) Methodology,

Survey 1 was prepared using specialist online software and designed along the lines of the Delphi method. The questions for this survey were of a generic nature as the intention was for Surveys 2 & 3 to explore resultant themes at a deeper level. To exploit the CyberROAD Cybercrime Survey a number of distribution methods were employed by project partners. These included the project website, a dedicated website, announcements via social media, and prompting by email to interested parties. The surveys were split into two versions: one for English speakers worldwide and the other translated into Polish and aimed at Polish users.

3) Macro to micro (world, Europe, Poland case specific)

For the purposes of the CyberROAD project it was decided that the greatest value would be obtained from a comparative study using participants worldwide but with a bias towards European citizens. Using the Delphi method for the surveys made it possible to drawdown in orderto probe further using selective criteria, if required. For a European project, it made sense to compare the region with others at a macro level i.e., world, and also at a micro level i.e., a specific country: Poland. Poland was selected because it is one of the larger EU countries and is also represented by a national CERT team (CERT Polska) in the CyberROAD consortium. The participation of a national CERT allowed for easier access to various statistics on the threats affecting Poland and good potential outreach to other entities in the country as well as the general public which is especially important when disseminating surveys.

4) *Initial findings*

Cybercrime was seen by survey respondents as a problem rooted primarily in economic interests and in technology.

One of the findings of the survey was that most respondents consider "better education of users of the Internet" as the single most important topic that should be researched in order to make the Internet a safer place (75% of respondents). "Improved technology for our networks and operating systems" scored the next highest in the very important category (only 58% viewed this as very important), while "better laws and regulations" were viewed as very important by only 40%. Most respondents, however, rated “Better metrics and statistics on cybercrime” as their 2nd choice after selecting their top choice of topic for more research.

Indeed, the above responses seem to correlate with the response to another question, concerning training within their organization: 59% of respondents were not trained in cybersecurity issues at all or only if there was a problem (note: we included "don't know" responses in this category as well).

Even though many respondents considered cybercrime to be a concern and many had been victims either personally or as part of their organization (as many as 78%) most respondents declared that the main consequence of the cybercrime action was inconvenience (50% of respondents). Nevertheless, many claimed enormous losses to their country or worldwide economy as a result of cybercrime in general (although the most respondents said they had no idea what the losses where). It is unclear where these numbers are from, but it is worth noting that these were the highest possibilities in the question that they could choose from. Perhaps this seemingly contradictory response (large losses vs the primary loss being inconvenience) is due in part to the term ‘cybercrime’ being often understood in very different ways, as other responses in the survey indicated.

Another very visible problem is the relatively low reporting rate of cybercrime to the Police (44% of cybercrime cases not reported) and/or national CERTs (72% of cybercrime cases not reported). This is followed up by a low successful prosecution rate: only 8% of the cases were successfully prosecuted.

Information sharing in general was found to be a problem (only 43% respondents said they or their organization shared information on cyber-attacks) - an issue that also hinders effective measurement of cybercrime.

The responses to the Polish survey (the same survey but translated into Polish) were in many aspects similar, but in general tended to show slightly worse results in regard to user awareness and experiences with cybercrime. In part, this is possibly because the responder base was nearly the opposite of the English speaking one (consumer group vs a more specialist group). A comparison of Poland vs world statistics will be the subject of further research.

Overall, however, the initial findings appear to confirm that there is a tangible need for better definitions, metrics and statistics for cybercrime together with more training. Initial analyses tends to support the view that current definitions on cybercrime are confusing to stakeholders whose experiences do not align with the information readily available. This mis-match of messages is a stumbling block in cybercrime prevention which could be alleviated with better quantification. This area requires further investigation.

IV. Review of the State-of-the-Art of the Metrics and Economics of Cybercrime

Within the last 5 years (2011 to Jan 2015) there are 3,920 web searchable scholarly articles, papers and books relating to the ‘economics or costs of cybercrime’[6]. Added to this is the wide spectrum of commercial sources collecting, collating and disseminating related information and data, some of which is not publically accessible.

An in-depth comparative study of all relevant reports is outside the remit of the CyberROAD project and instead a sample of typical studies and reports were reviewed.

The five major studies on the theme of the ‘cost of cybercrime’ were selected as representative of their genre, together with one quantitative study with a focus on a specific attack type, and one study that specifically tackles the issue of

[6] Google search on 13.02.15

the cost of privacy, the related cost of identity theft and data breaches relating to personal data. The studies either present a breakdown on the 'cost of cybercrime', offer recommendations and advice on how costing and metrics can be improved or convey specific quantitative data. The studies selected come from academia, consumer groups, technology providers and policy advisors and align to the criteria of the CyberROAD Triad approach.

This short overview reveals commonalities among the studies, if not their methodologies, which point the way to a number of identifiable research gaps. Firstly, the degree to which data is considered as open and publically accessible depends on the viewpoint. The intended motive and aims of the data provider, which may altruistic in nature or commercially interested, is difficult to quantify. It follows that any related data is regarded with suspicion and its validity questioned; whose data can be trusted, how can a 'trusted' environment be measured? Methodologies used to collect and collate information can be unique to the entity, unclear or not fully disclosed. Data may be incomplete in the wake of a lack of standard modus operandi, guidelines on best practices or benchmarks for the measurement of data.

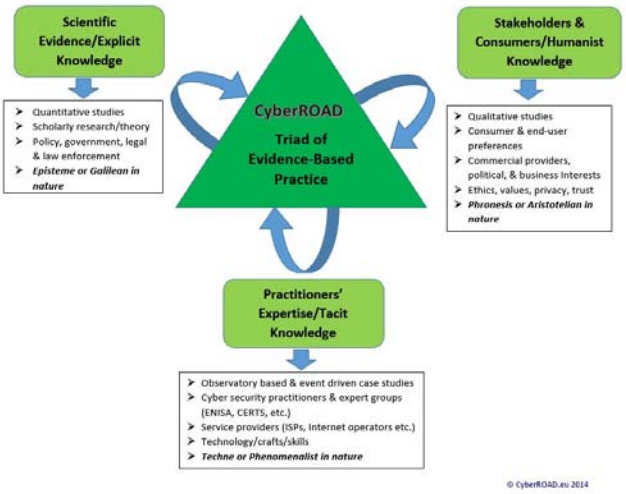

Fig 1. CyberROAD Triad of evidence-based practice - to validate all the choices made in cybercrime metrics and threat data

A. Anderson Et Al Study[10]

Although more than 100 different sources of data on cybercrime were counted in early 2012, the 'first systematic study of the costs of cybercrime' (Anderson 2012), concludes that available statistics are 'insufficient and fragmented' [11].The unequivocal message is that a lack of cohesion between different sources clouds the issue, leads to inconsistency of data and engenders mistrust of the numbers. As a consequence policy makers, who depend upon reliable figures, are left with little to go on, while the problem's true extent is obscured by the absence of easy-to-understand metrics. This report supports the widely held opinion that despite eye-catching headlines suggesting otherwise, it remains the case that few straightforward numbers exist on cybercrime and its true cost politically, economically, socially and morally.

This 'Cost of Cybercrime' study details a simplified framework for standardizing measurements, arrived at by decomposing an earlier, and much criticized [12], report from Detica [13], where 'difficult to assess' categories were used. Anderson et al suggest that 'cost to society' can be calculated through the application of 'sum of direct losses, indirect losses, and defense costs', to 'known data' on cybercrime and supporting infrastructures. The definition of cybercrime needs to have an integral baseline, from which the criteria for measurement is determined, and it is necessary for boundaries between traditional, transitional and modern crimes to remain flexible as society's dependence on cyberspace continues to increase. Using this method, the report claims that 'new computer crimes' actually cost only 'tens of pence/cents' per person and not the vast sums as reported elsewhere.

Within this study 'known data' consists of main types of cybercrime; online payment card fraud, online banking fraud, industrial cyber-espionage and extortion, fake antivirus, etc. Within the 'Infrastructure Supporting Cybercrime' grouping 'known data' is used on Botnets, Botnet mitigation by consumers, Botnet mitigation by industry, other botnet mitigation costs, and Pay-per-install. These are applied to one of four sections: Cost of genuine cybercrime, Cost of transitional cybercrime, Cost of cybercriminal infrastructure and Cost of traditional crimes becoming `cyber', and the category 'Criminal revenue' to direct/indirect/defense costs, is added to complete the framework. (See Fig 2)

Anderson et al conclude… 'Previous studies of cybercrime have tended to study quite different things and were often written by organizations (such as vendors, police agencies or music industry lawyers) with an obvious `agenda'.

Questions raised within this report provide several areas for further research, for example, what data can be trusted and from where should it be sourced, what are the determining metrics to be used, the need for benchmarks, why does cybercrime have high indirect costs and low indirect costs, (Anderson et al, p26). Additionally, Anderson et al conclude that less should be spent on '…anticipation of computer crime (on antivirus, firewalls etc.)', and more on '… catching and punishing the perpetrators'. This report sets a good precedent but further research is required in this area as a whole.

Type of cybercrime	UK estimate	Global estimate	Reference period	Criminal revenue	Direct losses	Indirect losses	Defense cost
	in million US dollars						
Cost of genuine cybercrime							
Online banking fraud							
- phishing	16	**320**	2007	x?	x?		
- malware (consumer)	4	**70**	2010	x↓	x↓		
- malware (business)	6	**300**		x↓	x↓		
- bank technology countermeasures	50	**1 000**	2010				x?
Fake antivirus	5	**97**	2008-10	x	x		
Copyright-infringing software	**1**	**22**	2010	x			
Copyright-infringing music etc	7	**150**	2011	x↓			
Patent infringing pharma	**14**	**288**	2010	x			
Stranded traveler scam	1	**10**	2011	x↓			
Fake escrow scam	10	**200**	2011	x↓			
Advance-fee fraud	**50**	1 000	2011	x↓			
Cost of transitional cybercrime							
Online payment card fraud	**210**	4 200	2010				(x)
Offline payment card fraud							
- domestic	**106**	2.100	2010				x↓
- international	**147**	2 940	2010				x↓
- bank/merchant defense costs	120	**2 400**	2010				x↓
Indirect cost of payment fraud							
- loss of confidence (consumes)	**700**	10 000	2010			x?	x
- loss of confidence (merchants)	**1 600**	20 000	2009			x?	x
PABX fraud	**185**	**4 960**	2011	x			x↓
Cost of cybercriminal infrastructure							
Expenditure on antivirus	**170**	3400	2012			x	
Cost to industry of patching	50	**1000**	2010			x?	
ISP clean-up expenditures	**2**	40	2010		x?		
Cost to users of clean-up	**500**	10 000	2012		x?		
Defense costs of firms generally	500	**10 000**	2010			x?	
Expenditures on law enforcement	**15**	400	2010			x	
Cost of traditional crimes becoming 'cyber'							
Welfare fraud	**1 900**	20 000	2011	x	(x)		
Tax fraud	**12 000**	125 000	2011	x?	(x)		
Tax filing fraud		5 200	2010	x	(x)		

Fig 2: Judgement on coverage of cost categories by known estimates (Anderson et al, 2012) [14

B. Ponemon Institute Study[15].

Since 2009, The Ponemon Institute has been conducting 'The Cost of Cyber Crime Study' The Ponemon Institute is an independent U.S.-based research group with the aim of informing the private and public sector on how to '…improve upon their data protection initiatives and enhance their brand and reputation as a trusted enterprise…' Ponemon Institute research is used by major corporations, U.S. federal and state departments, consumer groups and is widely publicized by a variety of media outlets. This report was sponsored by HP Enterprise Security.

The 2014 Ponemon Institute report is based on the findings from surveys conducted with 257 organizations using a cross-section of industry sectors in 7 countries – U.S.A, U.K., Germany, Australia, Japan, France and the Russian Federation. The research is field-based via interviews with senior-level personnel '...about their organizations' actual cybercrime incidents...' from large sized entities with more than 1,000 direct connections to the network or its systems (enterprise seats).

The total cost incurred by an organization is analyzed using criteria such as the 'costs to detect, recover, investigate and manage the incident response' along with costs that 'result in after-the-fact activities and efforts to contain additional costs from business disruption and the loss of customers' but excluding the cost of 'expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations'.

An initial comparison of the Anderson et al study to the Ponemon Institute report reveals an immediate and common problem within this field of inquiry. For example, both reports use valid research techniques but comparison is untenable as different criteria and methodologies are employed in gathering and collating the material. Here are two studies with the same title but with a diverse approach to the research matter. It is, therefore, unsurprising that the results are disparate.

The research gap uncovered here points to the use of 'difficult to assess' categories, a criticism levelled against the Detica study in Anderson et al's report, but could equally apply to a number of recent studies. Further research is needed to ascertain how much trust can be placed in figures that are hard to substantiate.

C. McAfee Annual Cybercrime Reports [16]

The McAfee report of June 2014 'Net Losses: Estimating the Global Cost of Cybercrime' reviews the accuracy of its own evaluation early on under the section header 'Estimating global loss from incomplete data' (page 04), 'International agreement on a standard definition of cybercrime would improve the ability to collect consistent data.' Despite this data accuracy warning, McAfee appraises that the inclusion of certain additional indirect costs, such as reputational damage, show the '…full effect of cybercrime on the global economy.'

Sources for this report range from the German Office for the Protection of the Constitution, the Netherlands Organization for Applied Scientific Research (TNO), China's Peoples Public Security University, the European Commission, the Australian Institute of Criminology Research, Malaysia's Chief Technical Officer, and estimates by government agencies in other countries and consulting and cybersecurity companies around the world.

McAfee aggregates data from sources within 51 countries '…who account for 80% of global income,' and uses what is 'publically available' from resources on IP theft, fraud, or recovery costs with additional field-based data from public servants and subject specialists. Adjustments are applied to account for regional differences and to arrive at an estimated global cost. The results for individual countries are available as separate reports.

The lack of effort made by most countries in collecting data on cybercrime losses, along with widespread inconsistencies and poor quality of the data that is gathered, is a re-occurring theme in this report. The three example methods used to 'extrapolate a global loss figure' highlight this very problem. Method 1 uses the loss by high-income countries to deduce a global total, method 2 totals the amount for all countries where open source data is available, and method 3 'aggregate costs as a share of regional incomes.' The report goes on to acknowledge the inadequacies of these methods which, due to the lack of reliable data, could either be an 'overestimate' or 'underestimate' of the true cost of cybercrime worldwide.

The research gaps presented by the McAfee report point directly to the lack of reliable data. Despite being a multi-national company with a global outreach, McAfee is unsure of its own results and deemed it necessary to express its doubts about the ability to collect and collate accurate and reliable data.

A further research gap relates to the role of the corporate entity in this field. Is it possible to assess whether information delivered from the private sector is always biased towards its own agenda? Many different types of organizations currently provide critical services and share data to help protect against

cyber-attacks. How can these be more effectively used, and trusted, to provide the types of figures that are missing. What can be done to improve the availability of data in countries around the world? Who can be trusted to provide this service in other countries? Should this be a role for a new, independent entity?

D. East West Institute Study [17]

One of the few global studies into the need for improved methods of measurement was undertaken in 2013 by the East West Institute (EWI), an international, non-partisan, not-for-profit policy organization that focusses on confronting critical challenges. 'Measuring the Cybercrime Problem' examines how trusted metrics and performance benchmarks can be established, and a trusted centralized data collection entity created, both research gaps previously identified in this review. The EWI study 'presents a bold solution to this problem that involves private sector leadership aimed at promoting trust and cooperation'. The report concludes with three recommendations and calls for '…volunteers from all sectors—ICT, energy, financial services, transportation, retail, medical and others…' to carry these out.

Existing information sharing entities are benchmarked against 'Target Criteria' (Figure 2) based on three key areas: Governance-Related, Breadth-Related and Information-Related. Results of the 'Gap Analysis' are reported in table format (Figure4). .

Table 1. Target Criteria Defining the Solution Space

	Governance-Related		Breadth-Related		Information-Related		
	Sector Leading	Motivation of Participants	Geographic	Infrastructures	Focus	Type	Objectives
Solution Space	private	voluntary	worldwide	full spectrum	incidents	quantitative	measurement

Figure 3: EWI Scope of Target Criteria

Commercial entities are excluded on the grounds that, '… they are seen as likely to try to influence market conditions, whether or not this perception is justified.' The resulting 'Gap Analysis' reveals that not a single entity reached all the Target Criteria, one achieved 5 out of 7, and 5 scored 4 out of 7, giving justification to EWI's call for the creation of a trusted entity for data measurement, as one could not 'be found'.

E. Applying the EWI Gap Analysis in CyberROAD

In Deliverable 2.1 Section 4.4.2 we outlined how CyberROAD would define its roadmap goals, using normative and explorative means, supported by available data such as partner CyberDefcon's observatory[7]. The EastWest Institute study shows the critical nature of quantitative data in the measurement of cybercrime costing. To test out the suitability of the observatory tool it was measured against the 'EWI Scope of Target Criteria'. The results are detailed in Figure 5.

	Governance-Related		Breadth-Related		Information-Related		
	Sector Leading	Motivation of Participants	Geographic	Infrastructures	Focus	Type	Objectives
Solution Space	private	voluntary	worldwide	full spectrum	incidents	quantitative	measurement
BITS	private	voluntary	U.S.	financial services	knowledge	qualitative	collaboration
Breach Notification	public	mandated	various governments	varies[24]	incidents	quantitative & qualitative	notification
CERTs	private or public	voluntary	national	full spectrum	threats	qualitative	alerts
CPNI	public	voluntary	U.K.	essential services	advice	qualitative	reduce vulnerability
FCC CSRIC	public	voluntary	U.S.	communications	threats, knowledge	qualitative	advice
DSCI	private	voluntary	India	began with IT, now expanding	surveys	qualitative	awareness
EBITT	private	voluntary	worldwide	full spectrum	policy	qualitative	promote business
ENISA	public	voluntary	EU	full spectrum	knowledge	qualitative	prevent problems
FIRST	private	voluntary	worldwide	ICT	incidents	qualitative	response coordination
FS-ISAC	private	voluntary	U.S.	financial services	threats	qualitative	prepare and respond
ICPC	private	voluntary	worldwide	GUCCI[25]	knowledge	quantitative & qualitative	protection, measurement
ISACs	private	voluntary	U.S.	multi-infrastructure	knowledge, threats	qualitative	awareness
ISC	industry[26]	voluntary	China	information and communications	knowledge & advice	quantitative & qualitative	policy
M3AAWG	private	voluntary	worldwide	information and communications	knowledge	qualitative	collaboration, improvement
NRSC	private	voluntary[27]	U.S.	communications	network outages	quantitative & qualitative	measurement, improvement
NSIE	public	voluntary	U.S.	communications	national security threats	qualitative	protection
Quest Forum	private	voluntary	worldwide	communications	quality	quantitative & qualitative	improvement
Spamhouse	private	voluntary	worldwide	unrestricted	spam messages	quantitative	track & fight spam
WARPS	private or public	voluntary	Europe	unrestricted	threats, incidents and solutions	qualitative	warn, advice and reporting

Attribute Relative to Solutions Space | Target | Outside

Figure 4: EWI Gap Analysis

The 'Global Security Map' surpasses the scores of every other entity used in the EWI sample but misses the target on 'Focus' when matched to the criteria determined by the Institute. In the context of CyberROAD the target criteria for 'Focus' would more appropriately be 'knowledge', as opposed to 'incidents', as this measure has more relevance to the needs of this project.. According to the criteria required in the CyberROAD project, applied to the EWI methodology in assessing the suitability of selected 'candidates', the 'Global Security Map' passes the 'trust' test. This exercise demonstrates two points: 1) The value of this type of methodology in matching a sample set against specific criteria, 2) Modifying the criteria in 'Focus' enables the EWI assessment tool to be applied according to individual requirements.

	Governance-Related		Breadth-Related		Information-Related		
	Sector Leading	Motivation of Participants	Geopgraphic	Infrastructures	Focus	Type	Objectives
Solution Space	private	voluntary	worldwide	full spectrum	incidents	quantitative	measurement
GlobalSecurityMap	private	voluntary	worldwide	full spectrum	knowledge	quantitative	measurement

Attribute Relative to Solutions Space | Target | Outside

Figure 5: EWI Gap Analysis used to assess the 'Global Security Map'

There may be value in widening the sample set to include corporate entities who are willing to be tested against set standards or benchmarked criteria to verify the quality of their data. Further research is needed into how similar tools can be used to assess the suitability of data providers according to need.

[7] http://globalsecuritymap.com

F. *Neustar UK annual DDOS Report [23]*

In May 2014 Neustar published its second annual 'UK DDoS Attacks and Impact Report'. Neustar began as an operating unit managing large datasets under Lockheed Martin, a global aerospace, defense, security and advanced technology company. Today, Neustar handles billions of DNS queries and millions of text messages and phone calls. The report is based on findings from Neustar's survey of 331 UK companies across a variety of industries including financial services, technology, retail, government/public sector, health care, energy/utility, telecommunications, e-commerce, Internet services and media.

The scope of the inaugural 2012 survey was further developed with additional questions for the latest report. Each question targets specific information and data builds into a year-on-year profile of DDoS patterns and related changes. Examples questions include: What are the sizes and velocities of DDoS attacks? How long are DDoS attacks lasting?, Are DDoS attacks a bigger or smaller threat to your business versus a year ago?, and, How often were you attacked?

This seems a simple yet effective way of gathering quantifiable information and a good example of how the data can be displayed in an easy-to-understand format.

Even though this report appears to provide a model template for measurement and metrics there are still a number of issues when tested by the EWI method of analysis. Straightaway, it seems that Neustar would not qualify as a 'trusted' data provider due to its for-profit status. So, to what extent can this data be trusted? In the absence of benchmarks or standards, this is an unknown entity. Further research is required in this area to establish the criteria for cross-industry best practices and benchmarks.

Private, public and non-profits may each have a role to play in improving measurement and metrics. Used in this way, metrics can point to security vulnerabilities and provide a valuable source for gap analysis research. The Neustar report specifically highlights the vulnerability of the DNS/NTP servers to amplification attacks, when there are server misconfigurations. As a vulnerability, this has been highlighted by several other sources[8]. Any data, no matter what the source, should be viewed as a potential valuable asset, and put to the test. Currently, the problem is not so much 'bad data' as a lack of testing of its worthiness.

G. *The Economics of Privacy (Acquisti et al. 2015)* [24]

This study provides an updated survey on the economics of privacy. The main focus is not on the abuse of personal data stored on computers, nor on data breaches, but on the *value* that can be attached to private data.

As soon as people consent to the use of their data for marketing purposes, than the value of the data can be associated to the gain that the user may acquire in terms of discounts or other privileges in their purchasing activities. On the other hand, when personal data is stolen or misused, than the task of assigning a cost based on worth is still an open problem.

This study clearly points out the three factors affecting the value of private data stored and shared over the Internet: individual responsibility, market competition, and government regulation. **Individual responsibility** requires awareness of the benefits and risks that sharing data brings in itself. **Market competition** exists to the extent to which to a value can be attached to this data. Finally, **governments can regulate** this market as it happens in other sectors.

At present, this topic is addressed in different ways in the EU and the US. While EU is steering towards government regulation on the management of private data, the US is drawing a framework that would allow different sectors to self-regulate this market. It turns out that no clear figure currently exists on the value of data breaches when related to individual data.

V. GAP ANALYSIS

An analysis of a small sample of the many studies available reveals a number of key areas where more research would be of major benefit. Despite the lack of a common methodology where a like-for-like comparison becomes problematic, it is possible to thematically group the exposed research gaps. In this study the groups form into five key areas. The key groups are:

a) Definitions/Taxonomy

b) Metrics

c) Trusted Data

d) Standards/Benchmarks

e) Threats/cybercriminal acts

At the centre and common to all groups is the issue of 'trust'. This develops as the major theme that inter-links the individual parts. Diagrammatically, 'trust' is the central pivot upon which everything else relies.

[8] http://www.pcworld.com/article/2013109/report-open-dns-resolvers-increasingly-abused-to-amplify-ddos-attacks.html

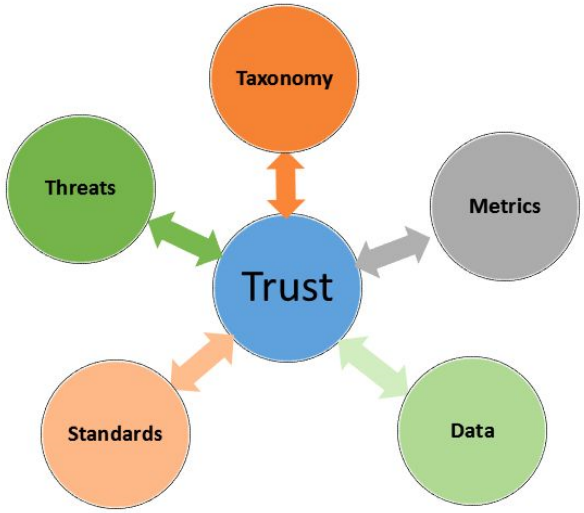

Figure 6: The Pivot of Trust

The groups surrounding the 'Pivot of Trust' provide a structured foundation for the study of the research gaps in relation to current scenarios. Each group is a worthy standalone subject in its own right. Groups may overlap to a larger or lesser degree and may be disproportionate in terms of the subject range and extent but, in terms of importance to Trust, each is of equal value.

As a scientific discipline, cybercrime is still in its infancy. Value can, therefore, be gained from the evolutionary experiences of other sciences. For example, research without some form of taxonomy would be chaotic in any area.

Accuracy of data is fundamental to other scientific research areas and is dependent upon tried and tested metrics for measurement. In some disciplines unreliable or untrustworthy data could be life threatening. With the advent of the Internet of Things, this could become a critical issue. Measurement is an essential, too, of risk assessment.

The issue of trusted data is emerging as an important topic as a result of this analysis. What trust is and how to quantify this is an element that has significant impact at ground-level involving perceptions as well as real events.

Trust and metrics are interwoven with the field of standards and benchmarks. Standards in industry are a cornerstone to improved safety, reliability and trust. Currently, this is not the case in the cybersecurity industry.

Initially, it would seem that the most importance place for more research would be in additional study of threats but it has emerged that this is only one of several key elements. More funds for study in this area are always welcomed but it is essential to know if the money is being spent on the right type of investigation. To know this with any certainty there has to be a greater understanding of the metrics and measurement of all disciplines.

A number of research gaps have been identified and grouped into themes as depicted in Fig. 6. The interplay of trust with each of these has also been highlighted. These themes will be investigated further during the course of the CyberROAD project. In the following sub-sections the importance of measuring economic costs on the state of cybercrime in 2020 is enumerated from current scenarios and weighed against some of the in findings from the CyberROAD Cybercrime Survey 1.

A. Current scenario

At present, the vast majority of governments addressed cyber security more within the framework of national defense rather than from the point of view of the protection of individual, social, end economic assets. We believe one of the main reason lies in the lack of clear figures on the real impact of computer incidents that prevents understanding

- The extension of the threat (i.e., number of computers, individual, enterprises, etc. that have been victims of attacks)
- The total loss that was caused by attacks, both in terms of tangible and intangible assets

In such a scenario, it is quite difficult if not impossible, to take decisions on

- The policies to set up in terms of education, training, awareness, as well as in terms of software and system verification and certification
- The money to spend to implement the above policies, are today quite limited as the real impact in terms of saving is not well defined.

In fact, laws and regulations need to be grounded on reliable data, that clearly shows how the money spent in prevention and monitoring actually decrease the likelihood of more serious consequences.

It turns out that the current scenario poses a serious threat as the lack of coordinated and focused actions from the legislative and government bodies paves the way for various forms of criminal activities that, if not properly tracked and recorded, does not provide evidence of the existence of a real threat.

B. Future scenario

A desirable future scenario is one in which governments can rely on solid methodologies to collect reliable figures about the real impact of cybercrime on companies, individuals and the public sector in order to take decisions, and allocate budget that is proportionate to the real threat.
In this scenario

- individuals, companies and the like have a high level of awareness on the possible uses of their data by public and private bodies, thus assigning a value to their data
- the market is mature enough so that a value can be assigned to each piece of information
- it is mandatory to disclose cyber-attacks and data breaches to a central authority, associating the costs incurred in terms of lost assets, lost business, repair/refactoring of software, and of business procedures.

- the above obligation implies that novel techniques are in place that allow assessing the influence of the attack and data breach

On the basis of past data, and of the actual market values, cost estimates are possible. Consequently, it is possible to devise policies that are cost-effective in containing the vulnerability of software and systems, handling security incidents, and preventing their rapid diffusion.

C Question of Trust

The notion of Trust is central in the security domain, as all the relationships among people, associations, companies, etc. are based on trust. Moreover, when decisions are to be taken on the policies needed to prevent security incidents, reliable information is needed on the probability of the events, on the data that can be targeted by attacks, and on the value of data loss and recovery. Consequently, sound metrics on the number of cybercrime events, their effects, and the damage that actually was caused from incidents is necessary for defence and recovery actions.

1) What is 'trusted' data?

Trusted data needs an agreed upon protocol for its acquisition, the measurements to be performed on the data, and the ways to securely store the data to prevent data pollution.

This chain can be enforced by clear national and supra national regulations that must require a uniform way for assessing the value of the assets in terms of data of companies, and the requirement to communicate any incident that has incurred, as well as a method for measuring the reach of the incident.

Incidents must be collected by a central point that ensures the correct processing of all data. This process in the EU is currently carried out by ENISA in an effort to provide for such trusted data. Metrics and protocols of communications still needs to be tailored in order to provide for data that should be not only complete, but also reliable.

2) Who can be 'trusted' with data?

The adherence to standardized metrics and protocols allows trusting the party that provides such data. In other words, the protocols for gathering, processing and sending data to the central authority should provide in itself a mean to assess the trust in those data.

3) The role of public sector / private sector /government/ governance, in information sharing

The experience in UK (cyber essentials) and in the USA (NIST CyberSecurity Framework) show that metrics and procedures have to be found by a joint effort of the private sector and the government. While the government acts as the central point for standardization of metrics and procedures that allows the production of official statistics, private companies must help devising the set of mechanism that can be actually implemented and represent the optimal trade-off between the cost of the solution and the data needed for the final assessment.

V CONCLUSIONS

Reliable data is a fundamental on which revenues and budgets rely from the top at government level down to board level and individual stakeholders. To understand a problem, to know what is and how to tackle it, is a task that presents greater challenges when size and extent of that problem remains very much shrouded in mystery. The CyberROAD project is working towards a roadmap for cybercrime and cyberterrorism to reveal the research gaps that can help policy makers make more informed decision on where money should be directed to return the best possible outcomes.

Cybercrime as a subject of study is still in its infancy and much can be learned from the evolutionary development of other recently established sciences. To begin, a clear taxonomy is an essential element from which a framework for further study can be developed. Our investigation of current and future scenarios via focused surveys and comparison of the cost of cybercrime reports reveals a number of research gaps that require attention if the scenarios outlined are to be achieved by 2020. Fundamental to the issue is the ability to quantify what we have and where we want to go. Currently, there is a mis-match between the experiences of stakeholders and the information to hand which can be improved with quantification of the issues and a reliable model for costing. Central to this information is the issue of trust, as without it there will be no confidence in the way forward with more time and money being wasted. Indeed, it is not an exaggeration to say that without quantification and measurement there will be no solution to the problem of cybercrime by 2020 or beyond.

VI. REFERENCES

[1] M. Levi, M. Innes, P. Reuter and R. V. Gundur, "The economic, financial & social impacts of organised crime in the European Union," Publication Office of the European Parliament, 2013.

[2] The Economist, "What's in a number? Estimating the cost of cybercrime," [Online]. Available: http://www.economistinsights.com/technology-innovation/analysis/measuring-cost-cybercrime/custom. [Accessed March 2015].

[3] C. f. S. S. (CSIS), "Cyber Threats and Information Security," Publisher CSIS Report, 2001.

[4] P. Horn, "It's Time to Arrest Cyber Crime," *Bloomberg Business,* 2006.

[5] McAfee & CSIS, "Stopping Cybercrime can positively impact world economies," 6 JUNE 2014. [Online]. Available: http://www.mcafee.com/uk/about/news/2014/q2/20140609-01.aspx. [Accessed 13 OCTOBER 2014].

[6] McAfee and CSIS, "Economic Impact Cybercrime 2," 2014.

[7] Group-IB, "Group-IB," 2011. [Online]. Available: http://www.group-ib.com/. [Accessed Oct 2014].

[8] IDC, "Security Products and Services," [Online]. Available:

http://www.idc.com/prodserv/maps/securityproducts.jsp. [Accessed Oct 2014].

[9] "Internet Live Stats," [Online]. Available: http://www.internetlivestats.com/internet-users/. [Accessed Mar 2015].

[10] The Radicati Group, Inc, "Email Statistics Report, 2015-2019 Executive Summary," 2015.

[11] "RIPE Network Co-ordination Centre," [Online]. Available: https://www.ripe.net/internet-coordination/press-centre/understanding-ip-addressing. [Accessed 20 March 2015].

[12] I. T. Union, "The World in 2014: ICT Facts and Figures," 2015.

[13] "Bots vs Browsers," [Online]. Available: http://www.botsvsbrowsers.com/. [Accessed March 2015].

[14] Barracuda Central, "Spam Data," [Online]. Available: www.barracudacentral.org/data/spam. [Accessed April 2015].

[15] Barracuda Central, "Web Data," [Online]. Available: http://www.barracudacentral.org/data/web. [Accessed April 2015].

[16] Spamhaus, "Spamhaus Block List," [Online]. Available: www.spamhaus.org. [Accessed Oct 2014].

[17] AV-TEST, "Malware," [Online]. Available: http://www.av-test.org/en/statistics/malware/. [Accessed April 2015].

[18] Akaimai, "Real-time Web Monitor," [Online]. Available: http://www.akamai.com/html/technology/dataviz1.html. [Accessed Oct 2014].

[19] "Squid Blacklist," [Online]. Available: www.squidblacklist.org/downloads.html. [Accessed Oct 2014].

[20] P. Institute, "2014 Global Report on the Cost of Cyber Crime," [Online]. Available: http://www.ponemon.org/. [Accessed Oct 2014].

[21] Shadowserver, "Malware," [Online]. Available: https://www.shadowserver.org/wiki/. [Accessed Oct 2014].

[22] HostExploit, "HostExploit World Hosts Reports," 2014. [Online]. Available: http://hostexploit.com/?p=reports. [Accessed April 2015].

[23] Neustar, "UK Annual DDOS Report," 2014. [Online]. Available: https://www.neustar.biz/ddos-attacks-report. [Accessed Mar 2015].

[24] C. T. a. L. W. Alessandro Acquisti, "The Economics of Privacy," *Journal of Economic Literature,* no. March 18, 2015, 2015.