This is a pre-print version of: Broadhead, Stearns. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180-1196. https://doi.org/10.1016/j.clsr.2018.08.005

The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments

Stearns Broadhead, Trilateral Research Ltd.
stearns.broadhead@gmail.com

Abstract
This article provides a multi-disciplinary overview of the contemporary cybercrime ecosystem and its developments. It does so by reviewing, synthesising and reporting on recent cybercrime research from fields such as cybersecurity, law and criminology. This article is divided into four main parts. The first part offers background on cybercrime and some of its main elements. It defines terminology, sets out a legal taxonomy of cybercrime offences and presents the estimated costs, threat agents and characteristics of various illicit activities and technical aspects of cybercrime. Parts two, three and four build on this preceding analysis by (separately) examining three prominent threat vectors within the ecosystem – malware, the darknet and Bitcoin and other cryptocurrencies. For each threat vector, the article identifies and investigates features, history, functions and current and expected states of development within the ecosystem. Through its attention to and synthesis of current research and results from different fields, this article offers a synoptic account of the cybercrime ecosystem, which can bridge potential knowledge gaps between fields.

Keywords: cybercrime, darknet, malware, Bitcoin, cryptocurrencies

Introduction
The continual transformation of the cybercrime ecosystem[1] remains a constant. The most serious threats, for example, change and sometimes change quite often. To appreciate such change, implement appropriate anti-cybercrime measures and take stock of recent and possible developments necessitates an up-to-date and synoptic picture of the cybercrime ecosystem and its various elements. One challenge in providing this, however, is that it requires awareness and expertise in different fields, not all of which are (necessarily) mutually intelligible to the different fields' experts. Policy and law enforcement priorities associated with stymying cybercrime can differ, at least in approach, scope or details, from those of a criminologist or infosec researcher. This article bridges such knowledge gaps between field experts and clarifies the current state of the cybercrime ecosystem by reviewing, synthesising and reporting in a clear way on current cybercrime research from multiple fields. Its central research question is: What is the current state of cybercrime (i.e., crime committed by means of or directed against computers or other forms of information communication technology – ICT)? This article answers this question by identifying some of the main elements of the cybercrime ecosystem, clarifying terminology, as well as reporting on recent findings of the costs, agents and characteristics of various activities and technologies. Furthermore, it (separately) examines three prominent threat vectors within the ecosystem – malware, the darknet and Bitcoin and other cryptocurrencies -- identifying and investigating their features, history, functions and current and expected states of development within the ecosystem.

The structure of this article is as follows. To orientate and ground the discussion of cybercrime trends, the first part (together with its various sub-parts) introduces terminology, classifies cybercrime offences, and identifies some of the costs and prominent threat agents within the ecosystem. The second part narrows the focus to malware and its most prevalent types in order to examine specific, widely used tools that facilitate illicit activities in the ecosystem. The next part examines various aspects of the darknet and cryptomarkets, which are prominent in enabling illicit activities and trade within the ecosystem. Following this is an examination of the exploitation of Bitcoin and other

[1] In this context, ecosystem means "a group of independent but interrelated [cyber or cyber-related] elements comprising a unified whole". *WordNet 3.0, Farlex clipart collection,* 2008. https://www.thefreedictionary.com/ecosystem

This is a pre-print version of: Broadhead, Stearns. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180-1196. https://doi.org/10.1016/j.clsr.2018.08.005

cryptocurrencies; the general aim being to identify how cryptocurrencies fit within and further illicit activities, such as those conducted via the dark net and by means of malware. This article ends with a brief conclusion that describes possible steps to counter the ecosystem's main threats.

1 Cybercrime: Definition, classifications, threat agents and costs

1.1 Definition and classifications

There is no single, universally adopted definition of cybercrime, a point acknowledged by academics[2] and organisations, such as Interpol[3] and actively debated in academic literature.[4] This article uses a working definition from Europol; namely, cybercrime is "any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT)".[5]

In addition to this working definition, there is an oft-used distinction[6] between senses of cybercrime. It first appeared in a background paper for the 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders[7]; namely,

> (a) Cybercrime in a narrow sense ("computer crime" [a.k.a. "cyber-dependent crime"]): any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them;
>
> (b) Cybercrime in a broader sense ("computer-related crime" [a.k.a. "cyber-enabled crime"]): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as possession, offering or distributing information by means of a computer system or network.

Even with this working definition and distinction, the types of legally prohibited conduct that fit within the cybercrime label can be specified. In accordance with Council of Europe's Convention on Cybercrime[8] (and its Additional Protocol[9]), a primary instrument of cybercrime prevention and enforcement, the categories of offences are:

> Offences against the confidentiality, integrity and availability of computer systems and data;
> Article 2 – Illegal access
> Article 3 – Illegal interception

---

[2] Viano, Emilio C., "Cybercrime: Definition, Typology, and Criminalization" in Emilio C. Viano (ed.), *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, Springer, Cham, Switzerland, 2017, p. 3.

[3] Interpol, "Cybercrime," 2017. https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

[4] The literature is sizeable and growing, but for a start cf. Alisdair A. Gillespie, *Cybercrime: Key Issues and Debates*, Routledge, New York, 2015.

[5] Europol, Internet Organised Crime Threat Assessment, 2017, p. 17. https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf

[6] Organisations such as Europol and ENISA commonly employ this distinction in their publications on cybercrime. As noted in square brackets in the quotation itself, current cybercrime literature tends to eschew the terms (a) "computer crime" and (b) "computer-related crime", opting instead for the synonymous: (a) "cyber-dependent crime" and (b) "cyber-enabled crime." *See*, for example, Europol, ibid, 12-3. Henceforth, this section will use the more current terms.

[7] United Nations, "Crimes related to computer networks: Background paper for the workshop on crimes related to the computer network", A/CONF.187/10, 3 February 2000. http://dag.un.org/bitstream/handle/11176/233350/A_CONF.187_10-EN.pdf?sequence=3&isAllowed=y

[8] Council of Europe, Convention on Cybercrime, ETS no. 85, 2001/2004. https://rm.coe.int/1680081561 . As of 22 December 2017, the Convention's number of ratifications/accessions totalled 56, including Council of Europe and non-Council of Europe states. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

[9] Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, 28 January 2003. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

Article 4 – Data interference
Article 5 – System interference
Article 6 – Misuse of devices
Computer-related offences (forgery, fraud);
Article 7 – Computer-related forgery
Article 8 – Computer-related fraud
Content-related offences;
Article 9 – Offences related to child pornography
Offences related to infringements of copyright and related rights;
Article 10 – Offences related to infringements of copyright and related rights
Acts of a racist and xenophobic nature committed through computer systems;
Article 3 – Dissemination of racist and xenophobic material through computer systems
Article 4 – Racist and xenophobic motivated threat
Article 5 – Racist and xenophobic motivated insult
Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity
Article 7 – Aiding and abetting.

The above classification provides statutory examples of offences. For the purposes of setting out a robust (if incomplete) typology of offences, the European Union's Directive 2013/40/EU[10] supplements the preceding. Thus, the cybercrime label also includes the following offences:

Article 3 – Illegal access to information systems
Article 4 – Illegal system interference
Article 5 – Illegal data interference
Article 6 – Illegal interception
Article 7 – Tools used for committing offences
Article 8 – Incitement, aiding and abetting and attempt.[11]

It bears repeating that the typological distinctions presented in this sub-section are a non-exhaustive sample of currently proscribed offences. Furthermore, the persistent transformation of the types and forms of cybercrime-related illicit activities and threats remains a weighty reason advocating against too restrictive a classificatory schema.[12] The introduction of these (working) definitions and typologies offers some initial terminological and conceptual clarity, which will help below when describing other elements within the contemporary cybercrime ecosystem.

1.2 Threat agents of cybercrime and other related illicit activities

The above definitions and associated classifications highlight types of crimes, but they do not identify the array of threat agents who commit them. To this end, attention sometimes narrowly focuses on organised crime groups (OCG)[13]; however, in the words of Broadhurst et al., "while many types of cybercrime require a high degree of organization and specialization, there is insufficient empirical evidence to ascertain if cybercrime is now dominated

[10] European Parliament and the Council of the European Union, Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14 August 2013, pp. 8-14. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN
[11] Ibid.
[12] Jerman-Blazic, Borka, and Tomaz Klobucar, "Towards the Development of a Research Agenda for Cybercrime and Cyberterrorism – Identifying the Technical Challenges and Missing Solutions", in Babak Akhgar et al., op. cit., pp. 158-60.
[13] The United Nations, Convention against Transnational Organised Crime (CTOC), General Assembly Resolution 55/25, 15 November 2000, Article 2(a) defines an organised criminal group (OCG) as "a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit". https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf;

by organized crime groups and what form or structure such groups may take".[14] Europol echoes this point in its 2017 IOCTA report and underscores that OCGs are more prevalent in certain types of criminal activities (e.g., key-card tampering and credit card skimming).[15] Current evidence indicates a variety of threat agents, including OCGs. This point does not undermine claims about the importance and prominence of OCGs within the cybercrime ecosystem, but rather contextualises their place within it.

Given the ever-shifting opportunities for criminal gain, the following typology of agents is a non-exhaustive sampling from current accounts.[16] Cybercrime is oftentimes transnational.[17] This fact increases the difficulty in detecting, locating and identifying offenders and thus reduces certainty about such categorisations[18]. In addition, various agent-side technical applications (e.g., VPNs) exacerbate attempts to attribute illicit acts to particular agents.[19]

Table 1 is based on 2016 and 2017 data and analysis from the European Union Agency for Network and Information Security (ENISA), *Threat Landscape Report 2016*[20] and the UK's *National Cyber Security Strategy 2016-21*[21], which classify threat agents based on identities, group affiliations, capabilities and motivations.

Threat Agent	Information
Individuals and small criminal groups[22]	**Description**: Capabilities and affiliations vary, but profit-seeking is the primary motivation for this category of agents – responsible for at least two-thirds of registered cybercrime incidents.[23] **Threat agents include**: – opportunistic offenders – habitual offenders and criminals.
Insiders	**Description**: Insiders are agents who threaten their organisations. The three sources of threats attributed to insiders are intentional (e.g., intentionally stealing an organisation's proprietary information), negligence (e.g., negligently exposing corporate login credentials to an unauthorised third-party) and error (e.g., mistakenly divulging company data to a third-party).[24] **Threat agents include**: – employees

[14] Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab and Steve Chon, "Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime", *International Journal of Cyber Criminology*, Vol. 8, No. 1, 2014, p. 2.
[15] Europol, op. cit., pp. 43-44.
[16] Kranenbarg, Marleen Weulen, André van der Laan, Christianne de Poot, Maite Verhoeven, Wytske van der Wagen and Gijs Weijters, "Individual Cybercrime Offenders", in Rutger Leukfeldt (ed.), *Research Agenda: The Human Factor in Cybercrime and Cybersecurity*, Eleven, The Hague, 2017, p. 25.
[17] World Economic Forum, Recommendations for Public-Private Partnership against Cybercrime, 2017, p. 5. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf
[18] Gercke, Marco, Understanding Cybercrime: Phenomena, challenges and legal response, ITU Publication, Geneva, 2014, p. 156.
[19] Kijewski, Piotr, Przemyslaw Jaroszewski, Janusz A. Urbanowicz and Jart Armin, "The Never-Ending Game of Cyberattack Attribution: Exploring the Threats, Defenses and Research Gaps", in Chen et al. (eds.), op. cit., p. 178.
[20] European Union Agency for Network and Information Security (ENISA), Threat Landscape Report 2016: 15 Top Cyber-Threats and Trends, Final Version 1.0, Heraklion, 2017. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport
[21] Especially, HM Government, *National Cyber Security Strategy 2016-21*, London, 2016, pp. 17-21. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
[22] Wall, David S., "Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime", *The European Review of Organised Crime*, Vol. 2, No. 2, 2015, p. 79.
[23] ENISA, op. cit., p. 69.
[24] Ibid., p. 69.

Threat Agent	Information
	– individuals (e.g., contractors) with access and/or credentials to Information and communications technology (ICT) of organisations
Organised criminal groups (OCGs)	**Description**: In keeping with the conventional definition from UN CTOC, OCG is a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences, in order to obtain, directly or indirectly, a financial or other material benefit.[25] **Threat agents include**: – traditional organised crime groups (ICT enhances OCGs' terrestrial criminal activities) – organised cybercrime groups (OCG with online-exclusive operations)[26]
State and state-affiliated agents[27]	**Description**: Such agents often operate for political, diplomatic, technological, commercial and strategic advantage, with a principal focus on the government, defence, finance, energy and telecommunications sectors.[28] **Threat agents include**: – Foreign intelligence services and agencies – State-sponsored individuals and small groups
Hacktivists	**Description**: Hacktivists typically select targets in response to perceived grievances or violations.[29] **Threat agents include**: – specific-issue-motivated individuals (e.g., Anonymous) – groups co-operating based on various events in an ad hoc manner
Cyberterrorists	**Description**: In keeping with the definition above, cyberterrorists are differentiated from other agents by their intention in acting. Current cyber terror activities are mainly concentrated in hacking, website defacements and hijacking of social media accounts; however, propaganda and planning attacks (especially via encrypted communication applications such as Telegram) are also major activities and threats.[30] **Threat agents include**: – pro-IS, al Qaeda and Boko Haram groups (or members of these terrorist groups)
Script kiddies	**Description**: These individuals typically use ready-made scripts or programs that can be found on the Internet to conduct cyberattacks, such as web defacements.[31] **Threat agents include**: – Young individuals (hence 'kiddies')

Table 1. Threat agents of cybercrimes

This table indicates not only the identities and affiliations, if any, of threat agents, but also their capabilities and, to a variable degree, motivations. The diversity of agents within the ecosystem belies two points of note not made explicit in the above table. First, future increases in cybercrime by entirely new threat agents such artificial intelligence systems[32] cannot be excluded. The table's snapshot of prominent agents, then, may (and estimably will)

[25] UN CTOC, op. cit., Art. 2(2).
[26] Choo, Kim-Kwang Raymond, and Peter Grabosky, "Cybercrime", in Letizia Paoli, *Oxford Handbook of Organised Crime*, Oxford UP, New York, 2013, p. 2.
[27] HM Government, op. cit., p. 18.
[28] HM Government, op. cit., p. 18.
[29] ENISA, op. cit., p. 70.
[30] Ibid., p. 71.
[31] HM Government, op. cit., p. 77.
[32] Straub, Jeremy, "Artificial intelligence cyber attacks are coming – but what does that mean?", *The Conversation UK*, 28 August 2017. http://theconversation.com/artificial-intelligence-cyber-attacks-are-coming-but-what-does-that-mean-82035

This is a pre-print version of: Broadhead, Stearns. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180-1196. https://doi.org/10.1016/j.clsr.2018.08.005

look different over time. To determine whether new agents enter the ecosystem calls for ongoing research and evaluation. Furthermore, novel threat agents with various, perhaps more extensive capabilities to cause harm underscore the need to allocate law enforcement resources for detecting and identifying new entrants in the ecosystem.[33] Second, individuals and small groups engaged in cybercrime for profit are currently the main source of cybercrimes.[34] This matter of financial gain and concomitant loss from cybercrime prompts questions and frames analysis of costs incurred from such illicit activities. The next step is to present some recent estimates in order to elucidate this matter of costs and provide a more complete view of the contemporary cybercrime ecosystem.

1.3 Costs of cybercrime

Despite ongoing academic debates and the lack of harmonisation of certain offences across jurisdictions[35], the preceding definitions and categories elucidate some core elements of the current cybercrime ecosystem. In addition to definitions and categories, tallying the costs of cybercrimes helps to illustrate extents and impacts. The ongoing transformation of cybercrime – wherein this year's most frequent computer crime may be next year's memory – means that such costs are perhaps best understood in a context of change.

There is a longstanding challenge in obtaining reliable and consistent quantitative data[36]. Anderson et al. capture the state of affairs well when they write:

> There are over 100 different sources of data on cybercrime, yet the available statistics are still insufficient and fragmented; they suffer from under- and over-reporting, depending on who collected them, and the errors may be both intentional (e.g., vendors and security agencies playing up threats) and unintentional (e.g., response effects or sampling bias).[37]

Among other things, this challenge can inhibit organisations', policy-makers', LEAs' and individuals' decisions about allocating resources for prevention, detection and remediation of cybercrime.[38] Furthermore, as described by Armin et al., the "lack of cohesion between different sources clouds the issue [and] leads to inconsistency of data and engenders mistrust of the numbers".[39] This challenge does not render efforts to measure and estimate cybercrime costs hopeless. In spite of the gaps in data and the reliability issues noted above, recent works by Dreyer (2018)[40], Riek et al. (2016)[41] and Romanosky (2016)[42], among others, provide measurement tools and models for estimating cybercrime costs and represent continued in-roads into the systematic accounting of costs.

Although there are variations across studies with respect to the particular breakdown or framework of what comprises costs (and thus what to measure), here the analysis of Anderson et al. will serve as a brief guide to help

---

[33] HM Government, op. cit., p. 12.
[34] ENISA, op. cit., p. 69.
[35] Viano, Emilio C., op. cit., p. 17.
[36] Viano, ibid.
[37] Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage, "Measuring the Cost of Cybercrime", in Rainer Böhme (ed), *The Economics of Information Security and Privacy*, Springer-Verlag, Berlin, 2013, p. 267.
[38] Wolff, Josephine, and William Lehr, "Degrees of Ignorance about the Costs of Data Breaches: What Policymakers Can and Can't Do about the Lack of Good Empirical Data", Working paper, 31 March 2017, p. 3. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3021414_code1832498.pdf?abstractid=2943867&mirid=1
[39] Armin, Jaart, Bryn Thompson and Piotr Kijewski, "Cybercrime Economic Costs: No Measure No Solution", in Babak Akhgar and Ben Brewster (eds.), op. cit., p. 140.
[40] Dreyer, Paul, *Estimating the Global Cost of Cyber Risk Calculator*, Santa Monica, CA, RAND Corporation, TL-281-WFHF, 2018. https://www.rand.org/pubs/tools/TL281.html
[41] Riek, Markus, Rainer Böhme, Michael Ciere, Carlos Gañán, Michel van Eeten "Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries", in *Proceedings of the Workshop on the Economics of Information Security (WEIS)*, University of California at Berkeley, 2016. http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_54-2.pdf
[42] Romanosky, Sasha, "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, Vol. 2, No. 2, 2016.

conceptualise the matter. Anderson et al. identify five types of costs: (1) criminal revenue (i.e., "the monetary equivalent of the gross receipts from a crime"[43]), (2) direct losses (i.e., "the monetary equivalent of losses, damage, or other suffering felt by the victim as a consequence of a cybercrime"[44]), (3) indirect losses (i.e., "the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out, no matter whether successful or not and independent of a specific instance of that cybercrime"[45]), (4) defence costs (i.e., "the monetary equivalent of prevention efforts"[46]) and (5) costs to society (i.e., "the sum of direct losses, indirect losses, and defence costs"[47]).

With these costs in mind, and with the previous description of data gaps as a general caveat, the figures below offer a sense of recent cybercrimes' costs within the cybercrime ecosystem. The figures below come from a survey of enterprise organisations conducted by the Ponemon Institute (working in conjunction with Accenture).[48] The figures present descriptive data of "actual costs incurred either directly or indirectly as a result of cyberattacks actually detected".[49] FY 2017 data was collected from respondents from 254 enterprise organisations in 15 sectors from seven countries – the United States, Germany, Japan, Australia, Italy, France and the United Kingdom.[50] Ponemon gathered data via 2,182 interviews from key individuals in respondent organisations and used a proprietary benchmark instrument for data analysis. The number of respondents per fiscal year (FY) were: n=254 (FY 2017); n=237 (FY 2016); n=252 (FY 2015).[51] With respect to Ponemon's survey, it should be noted that, in the words of Wolff and Lehr, "because its results are reported in aggregate, [it] offers no opportunity for any incident level analysis"[52]. So, these figures only aid in characterising some of the costs within the cybercrime ecosystem.

Figure 1 presents the total average annualised costs of cybercrime (FY 2016 and FY 2017) in US dollars from enterprise organisations in seven countries. Ponemon determined these costs by asking organisations "to report what they spent to deal with cyber crimes experienced over four consecutive weeks. Once costs over the four-week period were compiled and validated, these figures were then grossed-up to determine the annualized cost"[53]. Organisations from France and Italy did not participate in the Ponemon survey in FY 2016; hence, there is no data for them for FY 2016 (per the report, FY 2016 is presented as the FY 2017 total). As indicated in the figure, enterprise organisations in Australia report the lowest total average costs for FY 2017 at $5.41 million; they also reported the lowest in FY 2016 at $4.30 million. Conversely, organisations in the United States reported the total average annual costs of cybercrime for FY 2017 as $21.22 million and $17.36 million for FY 2016.

---

[43] Anderson, et al., op. cit., p. 269.
[44] Ibid., p. 270.
[45] Ibid., p. 271.
[46] Ibid., p. 272.
[47] Ibid.
[48] Ponemon Institute LLC, *2017 Cost of Cybercrime Report: Insights on the Security Investments that Make a Difference*, 2017. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50
[49] Ibid., p. 49. In contrast to those described by Anderson et al., Ponemon states on page five of its report that it examines actual costs defined as those "total costs organizations incur when responding to cyber crime incidents. These include the costs to detect, recover, investigate and manage the incident response. Also covered are the costs that result in after-the-fact activities and efforts to contain additional costs from business disruption and the loss of customers. These costs do not include the plethora of expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations."
[50] Ibid., p. 42.
[51] Ibid., p. 54. For a complete description of research methodology, see ibid., pp. 43-55.
[52] Wolff and Lehr, op. cit., p. 21.
[53] Ponemon, op. cit., p. 13.

This is a pre-print version of: Broadhead, Stearns. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180-1196. https://doi.org/10.1016/j.clsr.2018.08.005

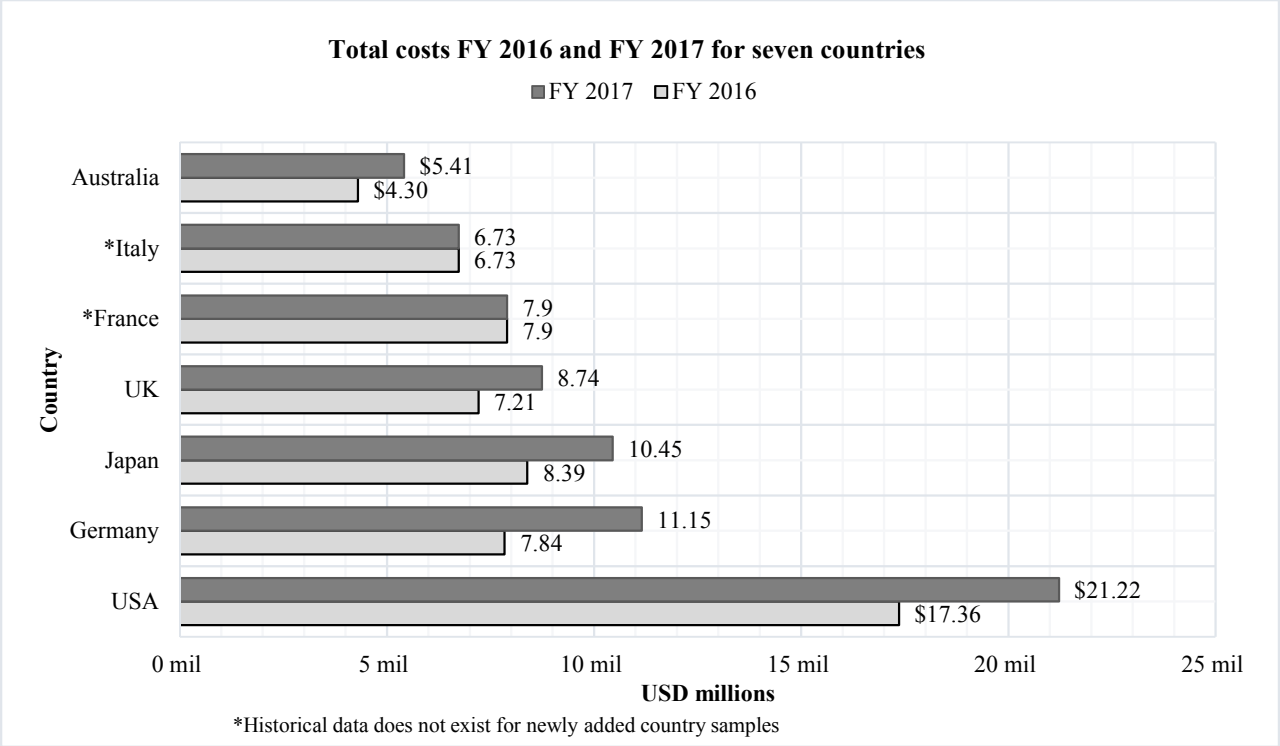

Figure 1. Cost of cybercrime for businesses ─ Total costs FY 2016 and FY 2017 for seven countries

Figure 2 indicates the percentage increase from FY 2016 to FY 2017 of the total annual costs of cybercrime reported by enterprise organisations participating in Ponemon's survey. Germany stands out in having the highest one-year increase, while the UK's increase was the lowest. Lacking FY 2016 data for organisations from France and Italy, the figure excludes these countries.

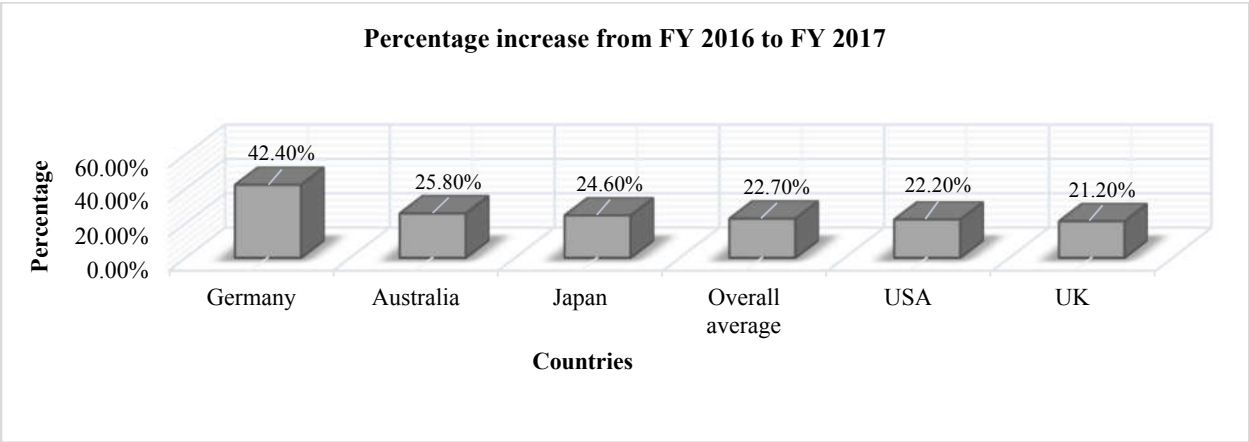

Figure 2. Cost of cybercrime for businesses ─ Percentage increase from FY 2016 to FY 2017

Figure 1 presents the total average annualised (FY 2017) cost of cybercrime (in US dollars) by industry sector as reported in Ponemon's survey. As this figure indicates, financial services bore the greatest cost due to cybercrime – $18.28 million – while the hospitality sector on average had the lowest cost at $5.04 million.

This is a pre-print version of: Broadhead, Stearns. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180-1196. https://doi.org/10.1016/j.clsr.2018.08.005

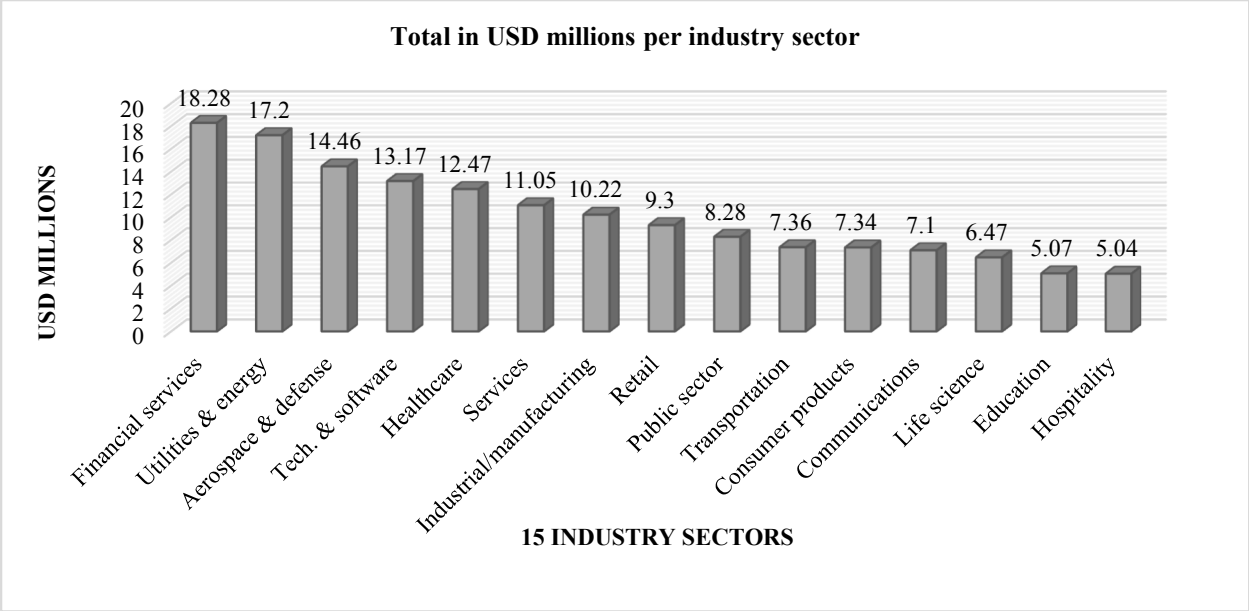

Figure 1. Cost of cybercrime for businesses ─ Total per industry sector

Figure 4 presents the percentage totals from FY 2015 to FY 2017 of four primary consequences of cybercrime – business disruption, information loss, equipment damage and other costs. Each consequence per FY is represented as a percentage of the total annualised cost (in US dollars) borne by all organisations.

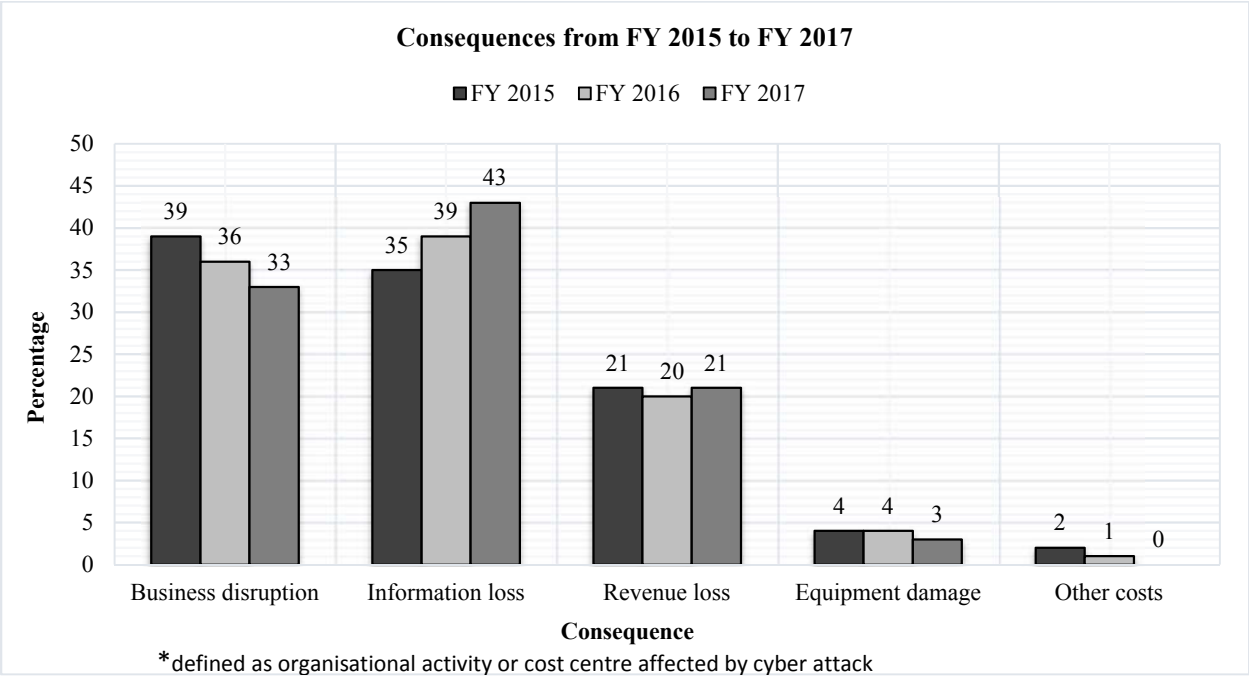

Figure 4. Cost of cybercrime ─ Consequences from FY 2015 to FY 2017

As stated above about the costs of cybercrime, the above figures present a broad characterisation of costs: they shed some light on the scope of financial burdens due to cybercrime. In concluding this section, it bears repeating that the broader scope of analysis within this section – terminology, typologies, agents and costs – helps to orientate and ground the following sections examining other specific aspects of the cybercrime ecosystem.

This is a pre-print version of: Broadhead, Stearns. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180-1196. https://doi.org/10.1016/j.clsr.2018.08.005

2 Malware

2.1 Definitions and prevalent types identified

The preceding sub-section and its constituent parts broadly sketched some of the main elements of the cybercrime ecosystem. The following sub-section narrows the focus to a single topic – malware. Malware is a notable illicit means by which threat agents generate revenue and threaten cybersecurity generally[54]. To detail how malware fits within the cybercrime ecosystem, as well as what it is and its deployment, this sub-section identifies and describes its currently prevalent types.

In accordance with the Directorate General for Internal Policies of the European Parliament, malware is "any piece of software that is designed to damage or perform unwanted actions on a computer system".[55] As described by Europol in 2017, "the two dominant malware threats encountered by EU law enforcement continue to be ransomware and information stealers".[56] Relying on data compiled from Europol in 2017 and analysis from other sources, Table 2 describes the six leading malware types in the ecosystem (in rank order of prevalence according to 2016 and 2017 Europol data).

Type	Information
Ransomware	**Description**: As defined by the United States Computer Emergency Readiness Team (US-CERT), "ransomware is a type of malicious software that infects and restricts access to a computer until a ransom is paid".[57] Collection of ransom payments typically relies on cryptocurrencies such as Bitcoin, making the subsequent laundering and monetisation simpler.[58] **Notable examples**: WannaCry, Bitpaymer, Reveton, CryptoLocker, Petya, NotPetya Bad Rabbit **State of threat within the ecosystem**: A major uptick in reports of ransomware across the world in 2016 and 2017, especially with the introduction of *WannaCry* and *NotPetya.*[59] As noted by ENISA, ransomware "delivered the most impressive growth [of malware threats] in all categories: number of campaigns, number of victims, average ransom paid, advanced of infection methods used, 'depth' of damage and turnover for cyber-criminals".[60]
Information stealers	**Description**: Information stealers typically appear as Trojans. Trojans generally consist of two parts: "a server side that runs on an attacked host and a client piece that runs on the attacker's console. The server code (usually kept very small in size, no more than a few KBs) is dispatched to the victim via some malware distribution method".[61] After installation of code to victim, observation of victim's activities – banking credentials or other valuable personally identifiable information (PII) – can result in access to victim's accounts, including e-mail, online bank, etc. **Notable Examples**: *Dridex*, *Ramnit* **State of threat within the ecosystem**: A persistent and significant threat given the frequency of use and access gained when successfully deployed.[62]
Mobile malware	**Description**: This type includes a wide variety of deployments. The most prevalent appearance in 2016/2017 was overlay malware, which displays fake overlays on a mobile device and captures user data that can be monetised by offenders. In January 2018, CheckPoint researchers observed three to

[54] Fanning, Kurt, "Minimizing the Cost of Malware", *Journal of Corporate Accounting & Finance*, Vol. 26, No. 3, 2015, p. 9.
[55] Directorate General for Internal Policies of the European Parliament, *The law enforcement challenges of cybercrime: are we really playing catch-up?* Study for the LIBE Committee P536.471, 2015, 17. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf
[56] Europol, op. cit., p. 19.
[57] United States Computer Emergency Readiness Team (US-CERT), "Ransomware: What it is and what to do about it?", Technical guidance document, 2017, p. 2. https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf
[58] Europol, op. cit., p. 19.
[59] Ibid.
[60] ENISA, op. cit., p. 43.
[61] Subrahmanian, V.S., Michael Ovelgönne, Tudor Dumitras and B. Aditya Prakash, *The Global Cyber-Vulnerability Report*, Springer, New York, 2015, p. 34.
[62] Europol, op. cit., p. 19.

Type	Information
	seven million downloads of *AdultSwine* malware, which injects illegitimate, pornographic ads into children's apps, via Google Play Store.[63] **Notable examples**: GM bot, SkygoFree, Adultswine **State of threat within the ecosystem:** Europol observed continued year-on-year increases in incidents, making this a growing threat.[64]
Exploit kit (EK)	**Description**: EKs install a malicious payload onto victim devices based on vulnerabilities found on those devices.[65] **Notable examples**: Neutrino; Nuclear; Angler; Blackhole.[66] **State of threat within the ecosystem**: The EK threat is still present; however, it has been reduced through industry-led actions, notably from Cisco, RSA Research and GoDaddy.[67]
Remote access trojans (RATs)	**Description**: RATs conform to the general description of Trojans but typically and additionally grant remote administrative control of users' systems. Such administrative access enables, for example, the installation of keyloggers, establishment of botnets and generally widespread access to users' data. Distribution of RATs often occurs via phishing e-mails and social engineering attacks.[68] **Notable examples**: Black orifice, MegalodonHTTP **State of threat within the ecosystem**: Europol regards this threat as serious because of its potential effects; however, Europol notes a decline in RATs in 2016.[69]
Counter antivirus services (CAV)	**Description**: CAVs (a.k.a. multi AV scanners or anonymous scanners) are web-based services that scan a piece of "malware against all of the Anti-Virus packages currently on the market to ensure it goes unnoticed when it is deployed against a victim's device".[70] **Notable example**: Refud.me **State of threat within the ecosystem**: Europol regards this threat as high given CAVs' use in the undetectable deployment of malware.

Table 1. Prevalent malware types in 2017

Two points, in particular, from the above table merit additional discussion. First, ransomware's growth represents a major development, noting again ENISA's description above. Although the origin of ransomware dates back to 1989[71], multiple enablers contribute to its recent rise[72]. According to Al-rimy et al., these enablers include: the availability of easy-to-use cryptography techniques, untraceable payment methods (i.e., cryptocurrencies), availability of ransomware development kits[73]. The extent of WannaCry, for example, launched on 12 May 2017 and infecting more than 230,000 computers in 150 countries[74], underscores, among other things, the potential for ransomware to generate revenue for threat agents. Second, the wide diffusion of mobile devices and users' reliance on them indicates the potential for this threat type to increase (e.g., in the number of incidents and the sophistication

[63] CheckPoint Research, "Malware Displaying Porn Ads Discovered in Game Apps on Google Play", 12 January 2018. https://research.checkpoint.com/malware-displaying-porn-ads-discovered-in-game-apps-on-google-play/
[64] Europol, op. cit., p. 20.
[65] ENISA, op. cit., p. 51.
[66] Europol, op. cit., 20.
[67] Ibid.
[68] Ibid.
[69] Ibid., p. 21.
[70] United Kingdom National Cyber Security Centre, *Cyber crime: understanding the online business model*, Report, 2017, p. 8. https://www.ncsc.gov.uk/content/files/protected_files/news_files/Cyber%20crime%20-%20understabnding%20the%20online%20business%20model.pdf
[71] Savage, Kevin, Peter Coogan and Hon Lau, "The evolution of ransomware", Security Response v1.0, Symantec Corporation, 6 August 2015, p. 7. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
[72] Al-rimy, Bander Ali Saleh Mohd Aizaini Maarof, Syed Zainudeen Mohd Shaid, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions", *Computers and Security*, Vol. 77, 2018, p. 147.
[73] Ibid, p. 148.
[74] Ehrenfeld, Jesse M., "WannaCry, Cybersecurity and Health Information Technology: A Time to Act", *Journal of Medical Systems*, Vol. 41, 2017, p. 104.

of malware used)[75]. It bears repeating that cybercrimes involving malware represent an important and, for threat agents, lucrative part of the cybercrime ecosystem. The next sub-sections focus on other elements within the contemporary ecosystem to provide a more complete view of its functioning and parts.

3 The darknet and cryptomarkets

3.1 Definition and distinctions

The darknet is a network "that is purposefully hidden; it has been designed specifically for anonymity . . . the darknet is accessible only with special tools and software — browsers and other protocol beyond direct links or credentials".[76] Such tools and software include "The Onion Router" (Tor) network and browser. The ready availability of illicit goods and services, coupled with near-anonymity, makes the darknet a key, if niche, part of the cybercrime ecosystem. The darknet is constantly changing, with vendors and underground markets frequently appearing and disappearing.[77]

There are distinctions between the darknet, deepweb and clearnet. The deepweb describes websites accessible through standard protocols (e.g., HTTP and HTTPS) that "are generally not indexed by major search engines due to security restrictions (such as additional password protection, CAPTCHAs, etc.)".[78] Benign and malicious activities occur on the deepweb with accessibility that is non-equivalent to the clearnet, the open portion of the Internet (a.k.a. clear web or surface web).[79] Locating sites on the deep web requires knowledge of specific URLs, as opposed to access via popular public search engines as on the clearnet.[80] The deepweb also includes closed (password-protected) corporate and university networks for student and employee access, websites such as Facebook, as well as library catalogues.[81]

3.2 Cryptomarkets – characteristics

The focus of this sub-section is cryptomarkets. A cryptomarket is "an online marketplace platform bringing together multiple vendors and listing mostly illegal and illicit goods and services for sale".[82] As Europol notes, cryptomarkets are "cross-cutting enablers" for various crimes.[83] Cryptomarkets are underground markets in the darknet which provide virtual spaces for trading illicit goods and services, such as malware (e.g., EKs, RATs) and ill-gotten financial data[84], which facilitate other crimes (cyber or otherwise).

Based on a sample of 103 cryptomarkets observed over a seven-year period (2010-2017), the EMCDDA and Europol reported that marketplaces remained active for an average of 8.5 months.[85] Included in this average were some resilient, enduring cryptomarkets – Valhalla, Dream Market and Outlaw Market – that operated for a mean of

---

[75] Fanning, op. cit., p. 12.
[76] European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol, *Drugs and the darknet: Perspectives for enforcement*, EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg, 2017, p. 77. http://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf
[77] Slobbe, Joost van, "The drug trade on the deep web: a law enforcement perspective", in European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), *The internet and drug markets*, EMCDDA Insights 21, Publications Office of the European Union, Luxembourg, 2016, p. 81.
http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf
[78] Robertson, John, Ahmad Diab, Ericsson Marin, Eric Nunes, Vivin Paliath, Jana Shakarian and Paulo Shakarian, *Darkweb Cyber Threat Intelligence Mining*, Cambridge UP, Cambridge, 2017, p. 6.
[79] EMCDDA, p. 135.
[80] Robertson, et al., op. cit., p. 15.
[81] Ibid., p. 15.
[82] Aldridge, Judith and David Décary-Hétu, "Cryptomarkets and the future of illicit drug markets", in EMCDDA, op. cit., p. 23.
[83] Europol, op. cit., p. 49.
[84] Ibid.
[85] EMCDDA and Europol, op. cit., p. 16.

just under 43 months.[86] The majority sampled, however, operated for no more than one year – the average being under four months.[87]

EMCDDA examined data on 89 cryptomarkets and found "exit scams" to be the most common reason for closure.[88] "Exit scams" consist of an operator abruptly shutting down a marketplace and absconding with currencies (e.g., Bitcoin) held in escrow for unfulfilled orders; thus, operators scam customers by suddenly disappearing.[89] "Voluntary exits", in which operators and users mutually consent to marketplace closure without losses, are the next most common cause of closure.[90] Law enforcement-based closures represent the third most common reason for market closing.[91] Hacks of marketplaces and de-anonymisation of participants were the fourth factor in marketplace closures.[92]

The technical demands for establishing and operating basic cryptomarkets are relatively low (at least in comparison with the next generation marketplaces described below); they require "hardware (such as a laptop), an operating system, e-commerce software, integration with a Bitcoin payment processor, and installation and configuration of Tor to provide a hidden service [i.e., cryptomarket] address at the web server".[93] In terms of development skills and maintenance efforts, this basic form of cryptomarket architecture is roughly equivalent to clearnet websites.[94] Resulting marketplace user interfaces can appear similar to popular clearnet e-commerce sites, such as Amazon or eBay.[95]

Next generation distributed marketplaces have begun to replace the above-described basic ones.[96] Unlike the basic type, where a sole operator may run an entire cryptomarket using a single or very few machines and servers, distributed cryptomarkets use software such as OpenBazaar that depend on all market participants' systems to host and, in some cases, handle transactions.[97] This model decentralises cryptomarket operation, reducing the risk of takedowns and the exposure of participants to de-anonymisation.[98] The distributed marketplace model poses an even greater technical challenge when attempting to locate, identify and attribute illicit and illegal activities to particular individuals.

The illicit goods and services offered on cryptomarkets are the core reason why the above-described architectures and technical characteristics of cryptomarkets focus on anonymisation. As Europol notes, the greater ability of LEAs, domain registrars and hosting providers to detect and respond to illicit clearnet trading (as opposed to that on the dark net) represents a primary *raison d'etre* for dark net marketplaces (i.e., they reduce external constraints to trade through identity protection).[99]

---

[86] Ibid.
[87] Ibid.
[88] Ibid.
[89] Ibid.
[90] Ibid.
[91] For notable instances of such closings, consider the 2017 closings of Alphabay and Hansa. Europol, "Massive blow to criminal Dark Web activities after globally coordinated operation", Press Release, 20 July 2017. https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation
[92] Ibid.
[93] Lewman, Andrew, "Tor and links with cryptomarkets" in EMCDDA, op. cit., p. 35
[94] Ibid.
[95] Aldridge and Décary-Hétu, op. cit., in EMCDDA, p. 23.
[96] Lewman, op. cit., in EMCDDA, p. 39.
[97] Ibid.
[98] Ibid.
[99] Europol, op. cit., p. 49.

This is a pre-print version of: Broadhead, Stearns. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180-1196. https://doi.org/10.1016/j.clsr.2018.08.005

3.3 Darknet markets – offerings

Based on data from Europol[100] and EMCDDA[101], Table 3 gives an overview of the main categories of illicit offerings (grouped by market below) on the darknet (in 2016 and 2017).

Market	Description
Drugs	The drugs market is the largest criminal market on the darknet. Of the total number of drugs listed on AlphaBay, Dream Market, Hansa, TradeRoute and Valhalla (from cryptomarket openings until 21 August 2017), 62% of listings were legitimate (i.e., non-counterfeit or fake items). Of this total, 77% of listings were for illicit drugs, 18% were for drug-related chemicals (e.g., raw material for refinement) and 5% were for pharmaceuticals.
Child sexual exploitation material (CSEM)	Given the nature of the material sold and the negative impacts on those exploited, this market represents a significant threat. CSEM is available via cryptomarkets, peer-to-peer networks and even the clearnet. However, Europol located only one cryptomarket dealing in CSEM – the majority of cryptomarkets disallow CSEM.
Cybercrime tools and services	Tools and services for cybercrime showed a 25% increase in number of listings by the end of 2016. (This increase was observed on AlphaBay). Of the tools and services offered there, listings for EKs and similar malware packages increased by 200%.
Counterfeit goods	Counterfeit goods violate intellectual property (IP) of genuine producers and/or designers. The wide availability of such goods available on the clearnet impacts the total percentage of listings on the darknet – between 1.5% and 2.5%. However, the most serious counterfeiting threat on the darknet is that of falsified identification documents (33% of all counterfeit listings) and bank notes (25% of all counterfeit listings).
Data	Compromised data, including banking credentials and other PII in various formats, represents a serious threat. Data is also one of the more common offerings on cryptomarkets. Europol observed an increase in the market for such data.
Weapons	Not all cryptomarkets list weapons (e.g., guns and armaments). For those marketplaces that do, such as Alphabay, this is a niche category. Given the impact for serious bodily injury resulting from use of weapons, however, the weapons market remains a major threat to security.

Table 2. Cryptomarkets – main illicit offerings by market

4 Exploitation of Bitcoin and other cryptocurrencies

4.1 Preliminaries on cryptocurrencies

A cryptocurrency is "a digital asset that is constructed to function as a medium of exchange, premised on the technology of cryptography".[102] Bitcoin is not the only example in the cryptocurrency universe. Its competitors include: Litecoin, released in 2011; Ripple, released in 2013; Monero, released in 2014; Ethereum, released in 2015; ZCash, released in 2016. Variations amongst them include differences in cryptographic algorithms, maximum number of coins circulated, institutional backing and degree of privacy-conferring features. Note that for the sake of brevity, at the cost of technical accuracy, this section assumes equivalent features and architectures amongst all cryptocurrencies, using Bitcoin as the baseline for characteristics discussed.

Bitcoin and other cryptocurrencies allow parties to transact (i.e., transfer value) without the need for a central authority, such as a bank, to verify the validity of transactions.[103] To enable such transactions and avoid double spending (counterfeiting), Bitcoin relies on a peer-to-peer network of computers ("nodes") to maintain and update

[100] Ibid, pp. 49-51.
[101] EMCDDA and Europol, op. cit., pp. 16-26.
[102] Chohan, Usman W., "Cryptocurrencies: A Brief Thematic Overview", UNSW Discussion Paper, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024330
[103] Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfede, *Bitcoin and Cryptocurrency: A Comprehensive Introduction*, Princeton UP, Princeton, 2016, p. 33.
[103] Nakamoto, op. cit., p. 1.

a publicly announced, distributed ledger (blockchain).[104] Michèle Finck succinctly defines blockchain as "an append-only decentralized database in which cryptographic algorithms verify the creation and transfer of data".[105]

Blockchain assures transacting parties of a coin's validity through an agreed upon and crypotographically proven history of the order in which the coin was used (i.e., a hash-based, proof-of-work system conducted through the peer-to-peer network).[106] When transferring coin, parties rely on cryptographic keys to sign transactions and mathematically prove the coin's origin (i.e., wallet owner) and prevent alteration of its history of use.[107] The transfer is broadcast to the network, which then validates and records the transaction.

Cryptocurrencies confer pseudo-anonymity to their users. With certain precautions (and with the limitations noted below), cryptocurrencies offer greater privacy protections than other forms of digital payments (e.g., credit card).[108] Bitcoin uses pseudonyms (i.e., Bitcoin addresses in the form of alphanumeric identifiers) that enable coin transfers to the appropriate recipient destination.[109]

Pseudo-anonymity does not mean unlinkability, however, whereby repeated interactions with a system cannot be traced back to the interacting user or users.[110] Public availability of transaction histories in the blockchain and the need for purchasers' real-life names and postal addresses for shipping influence levels of traceability. Furthermore, users may take privacy-enhancing measures to limit identity leakage. These measures include reliance on mixing services or tumblers (i.e., intermediaries who obfuscate transactions' traces), chain-hopping (i.e., converting into different virtual currencies) and not re-using Bitcoin addresses for different transfers.[111] Here, it should be noted that these privacy-enhancing measures can facilitate anonymous cash-outs of ill-gotten gains from activities such as successful ransomware deployments.

4.2 Exploitation of cryptocurrencies for illicit activities and state of the threat

This sub-section focuses on the exploitation of (and data estimates regarding) cryptocurrencies for illicit activities. As described above, the difficulty of tracing cryptocurrencies to users remains a primary reason for their continued use in transactions for illicit offerings and services on the clearnet and darknet. This is also one reason why cryptocurrencies pose an ongoing, serious threat within the cybercrime ecosystem. Although many activities on the darknet represent a serious threat within the ecosystem, the exploitation of cryptocurrencies for illicit activities extends beyond the darknet (or the illicit offerings and services such as those available on it). Especially in light of recent value rises of the currencies themselves, the theft of cryptocurrencies via hacks and ransomware comprise an increasing share of illicit activity.[112]

To get a sense of the general scope of illicit activities using Bitcoin via the darknet, consider Foley et al.'s recent study examining licit and illicit Bitcoin transactions and the users associated with them.[113] The authors collected a sample of 106 million Bitcoin users across eight years (2009-2017); these users collectively conducted

[104] Ibid.
[105] Finck, Michèle, "Blockchains and Data Protection in the European Union", Max Planck Institute for Innovation and Competition Research Paper No. 18-01, 2017, p. 1. https://ssrn.com/abstract=3080322
[106] Nakamoto, op. cit., p. 2.
[107] Karame, Ghassan, and Elli Androulaki, *Bitcoin and Blockchain Security*, Artech House, Norwood, MA, 2016, p. 59.
[108] Narayanan, et al., op. cit., p. 140.
[109] Ibid., p. 139.
[110] Narayanan, et al., op. cit., p. 139.
[111] Karame, op. cit., pp. 97-98.
[112] Chainanalysis, "The Changing Nature of Cryptocrime," Report, January 2018, p. 1; Moore, Tyler, Nicolas Christin and Janos Szurdi, "Revisiting the risks of Bitcoin currency exchange closure", *ACM Transactions on Internet Technology*, forthcoming, 2017, p. 1.
[113] Foley, Sean, Jonathan R. Karlsen and Tālis J. Putniņš, "Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?", January 2018. https://ssrn.com/abstract=3102645

approximately 606 million transactions.[114] Foley et al.'s data came from Bitcoin blockchain transaction records, data scraped from the darknet and police records of cryptomarket closures and seizures (e.g., those related to Silk Road's closure in 2013).[115] Using machine-learning algorithms, structural equation modelling and social network analyses, Foley et al. estimate with a 99% confidence interval that the proportion of users involved in illicit activities ranges from 21.73% to 28.76%.[116] Additionally, users engaged in illicit activities account for 44.33% of the share of total Bitcoin transactions, and they control around 38.21 % of Bitcoin addresses.[117] These estimates underscore the darknet's continued role in Bitcoin exploitation for illicit activities; however, the estimates should be treated carefully due to sampling issues such as potential duplication of observations, under-estimation of both legal and illicit users, non-coverage problems, as well as the inability of the models specified by the authors to clearly distinguish between legal and illicit users.

Foley et al.'s estimates of Bitcoin on the darknet indicate only one aspect of the abuse of cryptocurrencies. As described in preceding sub-sections and noted in the above introduction, ransomware attacks require payment in cryptocurrencies for restitution of users' compromised systems and data. A 2018 study by Huang, et al. indicates that between February 2016 and August 2017 (22 months), the ransomware families of Cerber, CryptXXX, CryptoDefense, Locky and WannaCry generated revenue (demanded in Bitcoin, but denominated by Huang et al. in US dollars) of $16,322,006 via 19,750 victim pay-outs.[118] It should be noted, as the authors themselves concede, this total represents a conservative estimate due to incomplete coverage.[119]

Of the five ransomware families examined by Huang et al., Locky proved the most lucrative for threat agents; it yielded a total of US$7.7 million over the 22-month observation period.[120] Cerber produced revenue of US$6.9 million; CryptXXX generated $1.87 million; CryptoDefense brought in a relatively trivial $70,000.[121] As described previously in this section, WannaCry is noteworthy in part because it affected a vast range of individuals and groups; it was also the focus of much media attention. Still, WannaCry brought in approximately $100,000, which seems slight compared to its notoriety.[122] Although Huang et al. excluded Cryptolocker from additional analysis, they nevertheless reported that it generated revenue of $2.05 million during the 22-month observation period.[123] These figures re-affirm a point consistently made in recent literature: the revenue-generating power of ransomware (and the success of attacks using it) suggest that it will continue to be a major source of cryptocurrency abuse and exploitation for illicit activities in the cybercrime ecosystem, a point corroborated by Europol.[124]

Cryptocurrency theft via hacks of third-party intermediaries that support cryptocurrency transactions and mining represents another prominent illicit activity in the cybercrime ecosystem.[125] Such intermediaries include currency exchanges used to convert cryptocurrencies into and from hard currencies and other virtual currencies, marketplace escrow services, cryptocurrency cloud mining marketplaces used to sell and buy hashing power, online wallets and mixing services.[126]

---

[114] Ibid., p. 11.
[115] Ibid., pp. 12–15.
[116] Ibid., p. 22.
[117] Ibid., p. 22.
[118] Huang, Danny Yuxing, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Kylie McRoberts, Elie Bursztein, Jonathan Levin, Kirill Levchenko, Alex C. Snoeren and Damon McCoy, "Tracking Ransomware End-to-end", 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, p. 8.
[119] Ibid.
[120] Ibid., p. 7.
[121] Ibid.
[122] Ibid.
[123] Ibid.
[124] Europol, op. cit., p. 19.
[125] Chainanalysis, op. cit., p. 1 and Moore, et al., op. cit., p. 1.
[126] Moore, et al., op. cit., p. 5.

This is a pre-print version of: Broadhead, Stearns. The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 34, No. 6 (2018), pp. 1180-1196. https://doi.org/10.1016/j.clsr.2018.08.005

According to data gathered and assessed by Chainanalysis, thefts via hacks account for approximately 847,000 Bitcoin to date.[127] A much-publicised and costly example of such theft occurred via the hack of the MtGox Bitcoin exchange from 2011 to 2013, which resulted in the loss of approximately 660,000 Bitcoins, which is approximately 80% of all Bitcoin stolen from 2011 to 2018.[128] To give a general sense of the value and frequency of cryptocurrency theft in the cybercrime ecosystem, the table below presents notable examples from 2016 to 2018 (in reverse chronological order), sourced from Chainanalysis and Tan and Nakamura.[129]

Date	Affected organisation and description of theft	Value (in coin and US dollar amount at the date of theft)
January 2018	Coincheck, a Japan-based cryptocurrency exchange, suffers a hack resulting in theft of funds.	523 million NEM coins or approximately $534 million
December 2017	Youbit, a South Korea-based currency exchange, loses 17 percent of its value and declares bankruptcy after a hack.	3,831 Bitcoin or approximately $73 million
	NiceHash, a Slovenia-based cloud mining marketplace, loses funds through theft via a compromised payment system.	4,450 Bitcoin or approximately $60 million
November 2017	Parity Wallet, an Ethereum client, suffers losses from theft due to a security flaw.	513,774.16 Ether or approximately $180 million
July 2017	CoinDash, an Israel-based exchange, suffered losses from theft via hack during ICO.	37,000 ethers or approximately $6 million
August 2016	Bitfinex, a crypto-currency exchange trading and currency-storage platform, suffered losses due to theft through a hack.	119,756 Bitcoin or approximately $65 million
June 2016	The DAO, a venture capital fund based on the Ethereum blockchain, suffers a hack and theft.	3.6 million Ether or approximately $50 million
May 2016	Gatecoin, a Hong Kong-based currency exchange, loses Bitcoin and Ethereum through a hack and theft.	185,000 ethers and 250 Bitcoins or approximately $2.14 million in total

Table 4. Notable cryptocurrency thefts (2016 – 2018)

The preceding numbers and analyses largely focus on Bitcoin, which was the near-exclusive cryptocurrency of choice for illicit activities in the cybercrime ecosystem in recent years.[130] As Europol notes, Bitcoin was the only currency accepted by the majority of cryptomarkets and for reconciliation of ransomware attacks.[131] Beginning in 2017, there was an uptick in use and acceptance of other cryptocurrencies: darknet markets began accepting Ethereum, ZCash and Monero, which provide greater user security and protections than Bitcoin.[132] Furthermore, as the table above indicates, theft of other (non-Bitcoin) cryptocurrencies also occurs.

The short and long-term prospects of specific cryptocurrencies, especially Bitcoin, remain uncertain. This is due in no small measure to volatility on the cryptocurrency market, with drastic fluctuations in currencies' values, as well as regulatory actions in some countries banning the use of cryptocurrencies.[133] Any uncertainty about specific coins does not apply to the use of cryptocurrencies generally for illicit activities and cybercrime. Europol regards

[127] Chainanalysis, op. cit., p. 6.
[128] Karpeles, Mark, "Announcement regarding the balance of Bitcoin held by the company", Press release, 20 March 2014. https://www.mtgox.com/img/pdf/20140320-btc-announce.pdf
[129] Chainanalysis, op. cit., pp. 6-8; Tan, Andrea and Yuji Nakamura, "Cryptocurrency Markets Are Juicy Targets for Hackers: Timeline", Bloomberg, 29 January 2018. https://www.bloomberg.com/news/articles/2018-01-29/cryptocurrency-markets-are-juicy-targets-for-hackers-timeline
[130] Europol, op. cit., p. 60.
[131] Ibid.
[132] Ibid.
[133] Lansky, Jan, "Possible State Approaches to Cryptocurrencies", *Journal of Systems Integration*, Vol. 9, No. 1, 2018, p. 24.

cryptocurrencies as an entrenched, cross-cutting enabler of criminal activity.[134] It bears repeating that the darknet represents a serious threat within the ecosystem, but illicit activities involving cryptocurrencies extend beyond the darknet. As the preceding estimates and analysis highlights, the revenue generated from ransomware and cryptocurrency theft suggest that such illicit activities are increasingly lucrative, persistent and serious threats within the cybercrime ecosystem.

Conclusion

As highlighted in this article, there is a diversity of fields from which research on cybercrime comes and bringing them together in a single overview helps to clarify for various field experts the ecosystem's interrelated elements. This article also showed that the elements within the cybercrime ecosystem sometimes rapidly transform and, as such, require the ongoing vigilance of LEAs, enterprise organisations, end users and others. In spite of the rapidity of change, there remain some general concluding points (drawn from the above-cited literature) to hold in mind. First, the harmonisation of cybercrime offences within and across jurisdictions can help to facilitate co-operation amongst various national, supranational and international agencies, organisations and institutions in their efforts to stamp out cybercrime. Second, the need for consistent quantitative data about various illicit activities within the ecosystem marks a known, if still unsettled issue. Concerted efforts to devise, adopt and apply standardised methods and metrics may aid in producing uniform accounts of the cost, scope and impact of illicit activities. Third, particular types of malware may rise or fall at various times; however, malware in its many guises remains (and presumably will continue to do so) a significant revenue source for threat agents and thus a significant threat within the ecosystem. Fourth, persistent monitoring and ever-advancing technical tools can help to quantify *and* combat the exchange of illicit goods and services on the darknet via cryptomarkets. Fifth, the exploitation of cryptocurrencies for illicit activities no longer pertains to the darknet alone; consequently, other abuses such as theft and ransomware require monitoring. Finally, even if a specific cryptocurrency may fall out of favour, cryptocurrencies in general represent an entrenched enabler of near-anonymous trade in illicit offerings. Consequently, these conclusions underscore the need for tools to detect and locate users involved in such transactions remains vital. The EU recognises this need and, among other ways of addressing it, funds the TITANIUM project, which began in May 2017, led by the Austrian Institute of Technology (AIT) with 14 other consortium members from Austria, Finland, France, Germany, the Netherlands, Spain and the UK, to research and develop tools to detect and counter illicit activities involving cryptocurrencies and darknet markets.

Acknowledgements

This article has been adapted from section 2 of the *Report on technical trends of Internet Organized Crime and Terrorism* that was prepared by the TITANIUM (Tools for the Investigation of Transactions in Underground Markets) consortium, of which the author was a member. The TITANIUM project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 740558. This article reflects only the author's views and the Commission is not responsible for any use that may be made of the information it contains.

The author wishes to thank David Wright, Rowena Rodrigues, Giuseppe Maio and Adriana Placani for their reviews and advice on various permutations of this article. The author also wishes to thank Svetlana Abramova, Marcus Riek and Nicholas Christin for their reviews and comments on section 2 of the TITANIUM project deliverable, *Report on technical trends of Internet Organized Crime and Terrorism*.

[134] Europol, op. cit., p. 60.

References

Abeslamidze, Sofiko. "North American Bitcoin Conference Stops Accepting Bitcoin for Tickets". *Coinspeaker*, 11 January 2018. https://www.coinspeaker.com/2018/01/11/north-american-bitcoin-conference-stops-accepting-bitcoin-tickets/

Akhgar, Babak, Andrew Staniforth and Francesca Bosco. *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Syngress, Waltham, 2014.

Akhgar, Babak, Michael Choras, Ben Brewster, Francesca Bosco, Elise Vermeersch, Vittoria Luda, Damian Puchalski and Douglas Wells. "Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism" in Babak Akhgar and Ben Brewster (eds), *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*. Cham: Springer, 2016.

Al-rimy, Bander Ali Saleh Mohd Aizaini Maarof, Syed Zainudeen Mohd Shaid. "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions", Computers and Security, vol. 77, 2018.

Aldridge, Judith and David Décary-Hétu. "Cryptomarkets and the future of illicit drug markets" in European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), *The internet and drug markets*, EMCDDA Insights 21, Publications Office of the European Union, Luxembourg, 2016. http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. "Measuring the Cost of Cybercrime", in Rainer Boehme (ed), *The Economics of Information Security and Privacy*, Springer-Verlag, Berlin, 2013.

Armin, Jaart, Bryn Thompson and Piotr Kijewski. "Cybercrime Economic Costs: No Measure No Solution" in Babak Akhgar, Michael Choras, Ben Brewster, Francesca Bosco, Elise Vermeersch, Vittoria Luda, Damian Puchalski, and Douglas Wells, "Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism" in Babak Akhgar and Ben Brewster (eds), *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, Cham, Springer, 2016.

Broadhurst, Roderic, Peter Grabosky, Mamoun Alazab and Steve Chon. "Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime", *International Journal of Cyber Criminology* 8 (1), 2014.

Chainanalysis, "The Changing Nature of Cryptocrime," Report, January 2018.

CheckPoint Research. "Malware Displaying Porn Ads Discovered in Game Apps on Google Play", January 12, 2018. https://research.checkpoint.com/malware-displaying-porn-ads-discovered-in-game-apps-on-google-play/

Chen, Thomas C., Lee Jarvis and Stuart Macdonald (eds). *Cyberterrorism: Understanding, Assessment, Response*. New York: Springer, 2014.

Chohan, Usman W. "Cryptocurrencies: A Brief Thematic Overview", UNSW Discussion Paper, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024330

Choo, Kim-Kwang Raymond and Peter Grabosky. "Cybercrime" in Letizia Paoli. *Oxford Handbook of Organised Crime*. New York: Oxford UP, 2013.

Savage, Kevin, Peter Coogan and Hon Lau, "The evolution of ransomware", Security Response v1.0, Symantec Corporation, 6 August 2015. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Council of Europe. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, 28 January 2003. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

Council of Europe. Convention on Cybercrime, ETS No.85, 23 November 2001. https://rm.coe.int/1680081561

Der Standard. "18-jähriger Wiener wollte Kind als Attentäter einsetzen". 7 January 2018. https://derstandard.at/2000071615313/Terroranklage-gegen-18-jaehrigen-Wiener-eingebracht

Directorate General for Internal Policies of the European Parliament. The law enforcement challenges of cybercrime: are we really playing catch-up? Study for the LIBE Committee P536.471, 2015. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536471/IPOL_STU(2015)536471_EN.pdf

Dreyer, Paul, Estimating the Global Cost of Cyber Risk Calculator, Santa Monica, CA, RAND Corporation, TL-281-WFHF, 2018. https://www.rand.org/pubs/tools/TL281.html

European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). *The internet and drug markets*, EMCDDA Insights 21, Publications Office of the European Union, Luxembourg, 2016. http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf

European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol. *Drugs and the darknet: Perspectives for enforcement*, EMCDDA–Europol Joint publications, Publications Office of the European Union, Luxembourg, 2017. http://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf

European Parliament and the Council of the European Union. Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14 August 2013, pp. 8-14. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN

European Union Agency for Network and Information Security (ENISA). Threat Landscape Report 2016: 15 Top Cyber-Threats and Trends, Final Version 1.0, 2017. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport

Europol. Internet Organised Crime Threat Assessment, 2017. https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf

Europol, "Massive blow to criminal Dark Web activities after globally coordinated operation", Press Release, 20 July 2017. https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

Fanning, Kurt, "Minimizing the Cost of Malware", *Journal of Corporate Accounting & Finance*, vol. 26, no. 3, 2015.

Finck, Michèle. "Blockchains and Data Protection in the European Union", Max Planck Institute for Innovation and Competition Research Paper No. 18-01, 2017. https://ssrn.com/abstract=3080322

Gercke, Marco. *Understanding Cybercrime: Phenomena, challenges and legal response*, ITU Publication, 2014.

Gillespie, Alisdair A. *Cybercrime: Key Issues and Debates*. New York: Routledge, 2015.

Hardy, Keiran and George Williams. "What is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism" in Thomas C. Chen, Lee Jarvis and Stuart Macdonald (eds), *Cyberterrorism: Understanding, Assessment, Response*. New York: Springer, 2014.

Hern, Alex. "Bitcoin's energy usage is huge – we can't afford to ignore it". *The Guardian*, 17 Jan 2018. https://www.theguardian.com/technology/2018/jan/17/bitcoin-electricity-usage-huge-climate-cryptocurrency

Hern, Alex. "Bitcoin's fluctuations are too much for even ransomware cybercriminals". *The Guardian*, 18 January 2018. https://www.theguardian.com/technology/2018/jan/18/bitcoin-fluctuations-ransomware-cybercrminals-malware-developers

Interpol, "Cybercrime," 2017. https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Jarvis, Lee, Lella Nouri, and Andrew Whiting. "Understanding, Locating and Constructing Cyberterrorism" in Thomas C. Chen, Lee Jarvis and Stuart Macdonald (eds), *Cyberterrorism: Understanding, Assessment, Response*. New York: Springer, 2014.

Jerman-Blazic, Borka and Tomaz Klobucar. "Towards the Development of a Research Agenda for Cybercrime and Cyberterrorism – Identifying the Technical Challenges and Missing Solutions" in Babak Akhgar and Ben

Brewster (eds), *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*. Cham: Springer, 2016.

Karame, Ghassan and Elli Androulaki, *Bitcoin and Blockchain Security*. Norwood: Artech House, 2016.

Kijewski, Piotr, Przemyslaw Jaroszewski, Janusz A. Urbanowicz and Jart Armin. "The Never-Ending Game of Cyberattack Attribution: Exploring the Threats, Defenses and Research Gaps" in Thomas C. Chen, Lee Jarvis and Stuart Macdonald (eds), *Cyberterrorism: Understanding, Assessment, Response*. New York: Springer, 2014.

Kranenbarg, Marleen Weulen, André van der Laan, Christianne de Poot, Maite Verhoeven, Wytske van der Wagen, Gijs Weijters. "Individual Cybercrime Offenders" in Rutger Leukfeldt (ed), *Research Agenda: The Human Factor in Cybercrime and Cybersecurity*. The Hague: Eleven, 2017.

Her Majesty's Government. *National Cyber Security Strategy 2016-21*, 2016, pp. 17-21. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Lewman, Andrew. "Tor and links with cryptomarkets" in European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), *The internet and drug markets*, EMCDDA Insights 21, Publications Office of the European Union, Luxembourg, 2016.

Maimon, David and Alexander Testa, "On the Relevance of Cyber Criminological Research in the Design of Policies and Sophisticated Security Solutions against Cyberterrorism Events," in (Gary LaFree and J. D. Freilich (eds), *The Handbook of the Criminology of Terrorism*, John Wiley & Sons, Hoboken, 2016.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://bitcoin.org/bitcoin.pdf

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfede. *Bitcoin and Cryptocurrency: A Comprehensive Introduction*. Princeton: Princeton UP, 2016.

Ponemon Institute LLC. *2017 Cost of Cybercrime Report: Insights on the Security Investments that Make a Difference*, 2017. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

Riek, Markus, Rainer Böhme, Michael Ciere, Carlos Gañán, Michel van Eeten. "Estimating the costs of consumer-facing cybercrime: A tailored instrument and representative data for six EU countries", in Proceedings of the Workshop on the Economics of Information Security (WEIS), University of California at Berkeley, 2016. http://weis2016.econinfosec.org/wp-content/uploads/sites/2/2016/05/WEIS_2016_paper_54-2.pdf

Robertson, John, Ahmad Diab, Ericsson Marin, Eric Nunes, Vivin Paliath, Jana Shakarian, Paulo Shakarian. *Darkweb Cyber Threat Intelligence Mining*. Cambridge: Cambridge UP, 2017.

Romanosky, Sasha, "Examining the costs and causes of cyber incidents", Journal of Cybersecurity, vol. 2, no. 2, 2016.

Slobbe, Joost van. "The drug trade on the deep web: a law enforcement perspective" in European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), *The internet and drug markets*, EMCDDA Insights 21, Publications Office of the European Union, Luxembourg, 2016. http://www.emcdda.europa.eu/system/files/publications/2155/TDXD16001ENN_FINAL.pdf

Straub, Jeremy. "Artificial intelligence cyber attacks are coming – but what does that mean?" The Conversation UK, 28 August 2017. http://theconversation.com/artificial-intelligence-cyber-attacks-are-coming-but-what-does-that-mean-82035

Subrahmanian, V.S., Michael Ovelgönne, Tudor Dumitras, B. Aditya Prakash. *The Global Cyber-Vulnerability Report*. New York: Springer, 2015.

United Kingdom National Cyber Security Centre. Cyber crime: understanding the online business model, Report, 2017. https://www.ncsc.gov.uk/content/files/protected_files/news_files/Cyber%20crime%20-%20understabnding%20the%20online%20business%20model.pdf

United Kingdom Parliament. An act to make provision about terrorism; and to make temporary provision for Northern Ireland about the prosecution and punishment of certain offences, the preservation of peace and the maintenance of order (a.k.a. Terrorism Act 2000), c.11, 2000. https://www.legislation.gov.uk/ukpga/2000/11/data.pdf

United Nations. Convention against Transnational Organised Crime, General Assembly Resolution 55/25, 15 November 2000. https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

United Nations. "Crimes related to computer networks: Background paper for the workshop on crimes related to the computer network", A/CONF.187/10, 3 February 2000. http://dag.un.org/bitstream/handle/11176/233350/A_CONF.187_10-EN.pdf?sequence=3&isAllowed=y

United Nations Office on Drugs and Crime. "Use of the Internet for Terrorist Purposes," Working Group Paper, 2012. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

United States Computer Emergency Readiness Team (US-CERT). "Ransomware: What it is and what to do about it?," Technical guidance document, 2017. https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

United States Department of Defense. "Terrorism," *United States Army Combined Arms Center*, 17 September 2008. http://usacac.army.mil/cac2/call/thesaurus/toc.asp?id=29533

Viano, Emilio C. "Cybercrime: Definition, Typology, and Criminalization" in Emilio C. Viano (ed), *Cybercrime, Organized Crime, and Societal Responses: International Approaches*. Cham: Springer, 2017.

World Economic Forum. Recommendations for Public-Private Partnership against Cybercrime, 2017. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf

Wall, David S. "Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime," *The European Review of Organised Crime*, vol. 2, no. 2, 2015.

Wolff, Josephine and William Lehr. "Degrees of Ignorance about the Costs of Data Breaches: What Policymakers Can and Can't Do about the Lack of Good Empirical Data", Working paper, 31 March 2017. https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3021414_code1832498.pdf?abstractid=2943867&mirid=1

Yannakogeorgos, Panayotis A. "Rethinking the Threat of Cyberterrorism" in Thomas C. Chen, Lee Jarvis and Stuart Macdonald (eds), *Cyberterrorism: Understanding, Assessment, Response*. New York: Springer, 2014.