INTELLIGENCE IN THE 21ST CENTURY

ANOTHER –*INT* ON THE HORIZON? CYBER-INTELLIGENCE IS THE NEW BLACK

Matteo E. BONFANTI *

Abstract

The pernicious nature of threats stemming from, or perpetrated through, the cyberspace is prompting the European and national decision-makers to adopt intelligence-led approaches for countering these threats. It pushes them to develop and employ targeted solutions to craft "cyber-intelligence" (cyber-INT) i.e. actionable knowledge of threat actors' intents and capabilities, as well as the vulnerabilities-opportunities they want to exploit. Similar to other cyber-related notions, there is no crystallised definition of "cyber-intelligence" (as a product and/or process) among both scholars and practitioners. Neither, it seems there are enough studies focusing on how it is crafted. In light of the above, the present paper tries to draw a clearer picture of this emerging practice by taking stock of the recently-promoted initiatives in the field and the existing analytical work on the topic. The paper starts by presenting the state of the art of cyber-intelligence programmes in the EU and in its Member States, and describes their recent developments. Then, it reviews the available scientific literature addressing cyber-intelligence. It discusses the notion of cyber-INT, examines how this intelligence is crafted through the lens of the (cyber) intelligence "cycle", and looks at the required capabilities (human, organisational and technological) for producing this kind of actionable knowledge. It concludes by sketching the main practical implications regarding the adoption of cyber-intelligence-led approaches, solutions and cooperation mechanisms across Europe.

Keywords*: Intelligence, Cyber-Intelligence, Cyber-Intelligence Process, Cyber-Security, Europe,*

Introduction

Since its foundation, the European Union (EU) and the Member States have supported the production and exchange of information and intelligence in order to enhance decision-making processes aimed at tackling targeted transnational security threats.[1] Aware that effective prevention of, and

* Senior Researcher Dr. *ETH Center for Security Studies, Zurich***,** matteo.bonfanti@sipo.gess.ethz.ch

[1] Arthur Gruszczak, *Intelligence Security in the European Union. Building a Strategic Intelligence Community*, (London: Palgrave-McMillian, 2016).

response to, menaces posed by terrorism, organised crime, natural or man-made disasters need to be knowledge/intelligence-based, European and national policy-makers have progressively promoted relevant actions and collaborations in this field. They have established new agencies and tasked them with intelligence functions, improved the collection and analytical capabilities of existing bodies, as well as encouraged the (bilateral and multilateral) flow of information and insight among peer security/law-enforcement organisations.[2] Nowadays, the pervasive and pernicious nature of threats stemming from, or associated with, the cyberspace seems prompting European and national authorities to intensify their actions and mutual cooperation with regard to the gathering and sharing of relevant information and intelligence.[3] It seems pushing them – and other stakeholders as well – to develop and employ targeted organisational, procedural and technological solutions to sustain the crafting of actionable knowledge that can be consumed for engaging in effective prevention and response.[4]

Cyber-threats are actual or potential dangers to the networks and infrastructures the cyberspace consists of, or to the availability, integrity and confidentiality of the information contained therein. They are also menaces perpetrated through the cyberspace to targeted individuals, organizations and communities in the physical/real domain. They might stem out from different sources, involve a multitude of actors, be exercised by using several tools, and consist in a wide and evolving range of activities.[5] Cyber-threats may generate from conducts perpetrated by State and no-state actors to achieve a wide

---

[2] At the multilateral level, cooperation has generally proven to be fragmented and limited. This is due to different but interrelated "friction" factors. See Matteo E. Bonfanti, "Collecting and Sharing Intelligence on Foreign Fighters in the EU and its Member States: Existing Tools, Limitations and Opportunities", in A. de Guttry, C. Paulussen, F. Capone, *Foreign Fighters under International Law and Beyond*, (The Hague: Springer, 2016), pp. 333-353; Den Monica Den Boer, "Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis" *Intelligence and National Security*, Vol. 30, 2015, pp. 402-419.

[3] There is no standard or universally accepted definition of "cyber-space" or "cyber-domain" (any spelling). The same goes for many other cyber-related terms *e.g.* "cyber-security", "cyber-threat", "cyber-attack", etc. Cf. https://ccdcoe.org/cyber-definitions.html. For the purpose of this essay, cyberspace is intended as a complex environment resulting from the interaction of several stakeholders, technologies, and practices. It is characterised by the processing of an ever-increasing wealth of information generated by the different activities that take routinely place in it.

[4] The reference to "actionability" is neither random nor trivial because it is what makes knowledge "intelligence".

[5] David Barnard-Wills & Debi Ashenden "Securing Virtual Space: Cyber War, Cyber Terror, and Risk", *Space and Culture*, Vol. 15, No. 2, 2012, pp. 110-123.

range of goals.[6] They may also originate from accidental events that compromise the correct functioning of, and accessibility to, information network infrastructures and systems. From a broader perspective, these conducts or events jeopardize the existence of those (State or non-state) organisations who rely increasingly, or are even critically dependent, on the information and services that are provided within or through the cyber-domain.[7] Having proper actionable insight into cyber-threats before/while they materialise can enable organisations to take preventive actions aimed at better safeguarding their interests and assets.

In Europe, a growing push towards the adoption of intelligence-led approaches/solutions for dealing with cyber threats comes from the members of the (not-formalised) European cybersecurity community. This community consists of representatives from supranational Institutions and agencies, domestic public bodies, private organisations, and the academia. Altogether, they contribute to shaping the discourse on cybersecurity in Europe and driving the actions that are taken within this policy area. The stakeholders of this community have already supported the definition and implementation of information/intelligence-led mechanisms for countering cyber-threats.[8] They have for instance sponsored the adoption of *ad-hoc* solutions for the delivery of "cyber-threat information/intelligence" (CTI), a product which should provide its consumers with the (technical) understanding of malicious networks operations and activities, and enable them to take subsequent actions.[9] However – at least as it is generally misconceived –, CTI alone does not prove to be fully suitable for enabling advanced prevention of cyber-

---

[6] *E.g.* State and State-sponsored actions may aim at gaining political, diplomatic, technological, commercial and strategic advantage; organised criminal groups generally aim at making illicit profit while terroristic networks o hacktivist have the goals of intimidating their victims or attract media attention.

[7] Nowadays, network and information systems and services – the Internet included – play a vital role in many contemporary societies. They have transformed, and are continuously shaping, the economic, social, institutional, and cultural life of several communities. Many of these systems are of public interest, and underlie the correct functioning of sensitive sectors of contemporary societies. This is, for example, the case of the automatic management and execution of processes that allow the functioning of critical infrastructures.

[8] Recently, EU Commission, "Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", Brussels, 2016, OJ C 75, 10.3.2017, pp. 124-128, par. 2.2.2.

[9] Sharing of threat information, current attack patterns, software vulnerabilities and so forth has been standardised in process through the establishment of a network of CSIRTs (Computer Security Incident Response Teams) and been augmented by the establishment and development of a number of initiatives such as STIX/TAXII, CyBox, MISPs (Malware information Sharing Platform). See, e.g., http://stixproject.github.io/supporters/.

threats.[10] This is due to the technical nature and strictly operational scope of cyber-threat information/intelligence that allows its consumers to understand network events and trends ("inside the wire perspective"), and adopt reactive measures. Generally, CTI products are not build, and do not provide knowledge, on the wider and articulated context within which cyber-threats are framed.[11] They do not grant the understanding of cyber-threat ecosystems and do not enable advanced prediction/prevention.

By endorsing the idea that organisations should move from reactive to proactive security management postures and disapproving the attitude to interpret cybersecurity mostly as "measures taken after-the-event" and "static perimeter defence", some members of the European cybersecurity community are now sponsoring the adoption of concepts, tools and practices for the crafting and sharing of a more all-encompassing intelligence on cyber threats.[12] This intelligence should enable its consumers to comprehend the operational, tactical and strategic contexts of the threats (agents, capabilities, motivations, goals, impact, and consequences not only from a technical perspective), foresee their developments on the short-mid-long terms, and take informed decisions on the preventive actions to be taken. If integrated in their security-related decision-making processes, it should enable organisations to assume "predictive and anticipatory rather than past-oriented", "dynamic than static", and "agile and quick adaptable than rigid and conformed" postures toward cyber-related perils. The above described intelligence is often labelled "cyber-intelligence" (cyber-INT or CYBINT) – or intelligence "from", "for" and "within" the cyberspace – to differentiate it from the technically-interpreted and narrow-scoped "cyber-threat information/intelligence". In general, the expression cyber-intelligence is used to convey the idea of a wide-scoped and better qualified knowledge of actual or potential events occurring in the cyberspace that may endanger an organisation.[13]

Similar to many other cyber-related notions, there is actually neither a crystallised definition nor a real common understanding of "cyber-intelligence"

---

[10] Brian P. Kime, "Threat Intelligence: Planning and Direction", accessed 1 September 2017 at https://www.sans.org/reading-room/whitepapers/threats/threat-intelligence-planning-direction-36857. As stressed by the author, Indicators of Compromise (IOCs) like virus signatures and IP addresses, hashes of malware files or URLs or domain names of botnet command and control servers are not by themselves intelligence. They are information useful for network static defence. *Ibidem*, p. 3.

[11] Cf. Michael Montecillo, "Why Context is King for Enterprise IT Security", April 2014 accessed 1 September 2017 at https://securityintelligence.com/enterprise-it-security-context-king/.

[12] The term "proactive" should be here understood as the capacity to address actual of potential cyber-threats by strengthening defence and response measures.

[13] See also *infra*.

(as a product and/or process) among policy-makers, practitioner organisations, scholars, and the public opinion. If one looks at the relevant policies or mechanisms that have been recently implemented at the EU and Member States levels as well as other documentation issued by private and public organisations and the academia, "cyber-intelligence" is not always comprehensively defined or definitions vary. Despite the growing use of this or similar expressions not only by the media but also scholars and practitioners (especially by cybersecurity vendors for marketing reasons), current thinking on the subject is limited or not well-developed.[14] This holds especially true if one looks at the academic or other intellectual works on the topic that have been so far produced in Europe.[15] A deeper investigation of the subject – both from a theoretical and practical standpoint – is missing. On the contrary, the academic and practitioners' reflection on cyber-intelligence is relatively more advanced among the US security and cyber-security stakeholders.[16] This could be the consequence of the earlier adoption of cyber-intelligence related concepts, practices and technological solutions by US-based organisations.[17] However, given that the push toward the adoption of cyber-intelligence programmes seems to be on the rise also within European cyber-security

[14] Sometimes, the use of the expression or reference to the concept of cyber-intelligence looks like an expedient for making a certain product appealing to potential consumers. Well, the same can be said about the present paper and its author's goal.

[15] At least this seems to be the case of part of the literature reviewed for the purpose of writing this paper. *Cf.* Mario Caligiuri, *Cyber Intelligence. Tra libertà e sicurezza* (Roma: Donzelli, 2016), Id., "Cyber intelligence, la sfida dei data scientist", June 2016, accessed 1 September 2017 at https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cyber-intelligence-la-sfida-dei-data-scientist.html, Antonio Teti, "Cyber Intelligence e Cyber Espionage. Come Cambiano i Servizi di Intelligence nell'era del Cyber Spazio" *Gnosis. Rivista Italiana d'Intelligence*, Vol. 3, 2013 pp. 95-121; Umberto Gori and Luigi S. Germani, *Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia* (Bologna: Franco Angeli 2012).

[16] Further to the literature that is cited *infra*, see also discussion that are held by US cybersecurity stakeholders on the Cyber Intelligence Blog available at https://cyberintelblog.wordpress.com/.

[17] See, *e.g.*, Office of the Director of National Intelligence, "The National Intelligence Strategy of the United States of America", 2014, pp. 1-24, accessed 1 September 2017 at https://www.dni.gov/files/2014_NIS_Publication.pdf. The strategy provides a definition of cyber-intelligence that reads as follow: "the collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, and operational activities and indicators; their impact or potential effects on national security, information systems, infrastructure, and data; and network characterization, or insight into the components, structures, use, and vulnerabilities of foreign information systems". *Ibidem*, p. 8. See also US Department of Defense Science Board, "Resilient military systems and the advanced cyber threat", January 2013, pp. 46 and 49, accessed 1 September 2017 at http://www.dtic.mil/docs/citations/ADA569975. Id., "The Department of Defence Cyber Strategy", April 2015, p. 24 accessed 1 September 2017 at https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

stakeholders, it would be worth deepening the discussion on this topic. In particular, it would be worth examining the notion of cyber-intelligence in more details as well as understanding the implications that may arise from the employment of cyber-INT-led approaches, methodologies, tools, and cooperation frameworks by the EU and national agencies and organisations.

The present paper intends to give a targeted contribution to the debate on cyber-intelligence. It tries to draw a clearer picture of this emerging practice by taking stock of the recently-promoted initiatives in the field and the existing analytical works on the topic. The paper starts by presenting the state of the art of cyber-intelligence programmes in the EU and in its Member States, and describes their recent developments. Then, it reviews the available scientific literature addressing cyber-intelligence. It discusses the notion of cyber-INT, examines how this intelligence is crafted through the lens of the (cyber) intelligence "cycle", and looks at the required capabilities (human, organisational and technological) for producing this kind of actionable knowledge. It concludes by sketching the main practical implications regarding the adoption of cyber-intelligence-led approaches, solutions and cooperation mechanisms across Europe. In general, the paper aims at two interrelated goals: improving the theoretical understanding of cyber-intelligence (academic-oriented goal), and outlining the broad issues regarding the promotion of cooperation on cyber-intelligence within the EU (practitioner-oriented goal).[18]

Cyber-intelligence and the Like across Europe

Often framed within the policy area of cybersecurity, different initiatives are presently promoted across Europe to sponsor the development and adoption of concepts, practices and technologies to timely identify, assess, prioritise and prevent existing or emerging cyber-related menaces.[19] Some of these initiatives make explicit use of the expression "cyber-intelligence" while others refer to the practice of generating actionable insight into cyber-threats through the collection, integration and analysis of both technical and broader contextual information about cyber-events. The notion of "contextual information" varies across the initiative at stake, its sponsors, their goals, as well as the type, object and scope of the crafted intelligence. In some cases,

[18] The paper arises from preliminary research activities that are currently carried out within a 3 years research project defined and run by author. Due to the limited number of pages here allowed and the early stage of the research project, the study will not go deep into all the salient issues that are identified.

[19] The EU cybersecurity architecture is described in EPSC Strategic Notes, "Building an Effective European Cyber Shield Taking EU Cooperation to the Next Level", Issue 24, 2017, p. 7, accessed 1 September 2017 at https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf.

contexts are drawn by processing further technical data on malevolent conducts (type of tool employed, vulnerability exploited, etc.) that affect organisations; in others, they are defined through information on the geo-political, socio-economic, and cultural environments where cyber-threats generate from.

At the European Union level, Institutions and agencies foster the production and sharing of intelligence on cyber-threats for two main purposes: (i) to protect the European networks and information infrastructures from incidents or attacks; (ii) to enforce the law, *i.e.* prevent and counter the criminal use of cyberspace.[20] The first purpose concerns networks and infrastructures that are employed both within the civilian and military domain. As per the latter, the EU 2014 Cyber Defence Policy Framework calls for the protection of Common Security and Defence Policy (CSDP) communication networks by strengthening "cyber threat assessment and intelligence capability to identify new cyber risks and provide regular risk assessments based on the strategic threat assessment and near real-time incident information coordinated between relevant EU structures and made accessible at different classification levels".[21] On the practical side, the European Union Agency for Network and Information Security (ENISA) and Europol provide (among other things) information and knowledge to support the EU institutions, Member States' authorities, and other stakeholder communities to enhance their cyber-threats awareness and prevention/response capabilities and actions.[22] While

[20] This reflects the EU cybersecurity policy and architecture that are structured around three pillars: network and information security, law enforcement, and defence. *Cf.* EU Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final, Brussels, 7.2.2013, p. 10 and 17.

[21] Cf. Council of the EU, "EU Cyber Defence Policy Framework, Brussels", 18.11.2014, pp. 7, accessed 1 September 2017 at https://ccdcoe.org/sites/default/files/documents/EU-141118-EUCyberDefencePolicyFrame.pdf.

[22] ENISA is a centre of expertise in cybersecurity in Europe who assists the Union institutions, bodies, offices and agencies and the Member States in adopting and implementing the policies in network and information security, as well as enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security incidents. Further to Members States ENISA cooperate with the private sector. See Regulation (EU) 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, Strasbourg, in OJ L 165/41, 18.6.2013, pp. 41-58. Europol is the EU's agency whose main goal is to support and enhance Member States' competent authorities action and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States. See Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council

ENISA's activities are mainly "IT-security management" oriented, Europol adopts law enforcement perspective and approaches to cybersecurity.

The former agency publishes – on yearly basis – the so called "ENISA Threat Landscape (ETL)" which offers an overview of identified cyber-threats, threat agents and current and emerging threat trends.[23] This (strategic) analytical product is mostly based on open source information even if some of the processed data are confidential. ETL aims to present the evolving cyber-threat environment and describe the top cyber threats and their components. It can be consumed by relevant organisations to define and plan new measures and security investments, as well as orient their existing cybersecurity strategies and actions. The content of ETL is referred to as "cyber-threat intelligence". Given the relevance of "contextual analysis" for the crafting of this product as well as its strategic scope, ETL should not be confused with the "narrow-scoped" threat information/intelligence (predominantly built upon IT-based data on artefacts/components). This is made evident by the methodology and models employed by ENISA to draft ETLs.[24] It is furthermore confirmed by the Agency itself when describing its position on CTI. As emerges from the 2016 ETL, the integration of contextual information and analysis is what the ENISA considers to be a necessary component to pass from "CTI information to knowledge".[25] However, within the ETLs crafting process, contextual information has specific meaning/scope. It covers the threat agents, their resources, modus operandi, used artefacts, threat positioning thorough the kill chain, related threats, evolving trends, and mitigation actions. In the ENISA's perspective these pieces of information and their interconnections make up the context of cyber-threats. As one may see, the

---

Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, Strasbourg, in OJ L 135, 24.5.2016, p. 53-114.

[23] Moreover, every year thematic threat landscapes are developed. These analytical reports present the cyber-threat exposure of particular sectors/application areas and propose mitigation strategies based on existing good practices. Further info at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends. See for example, ENISA, Big Data Threat Landscape and Good Practice Guide, January 2016, accessed 1 September 2017 https://www.enisa.europa.eu/publications/bigdata-threat-landscape.

[24] Cf. ENISA, Threat Landscape Report 2015, Ch. 2.1; Threat Landscape Report 2014, Ch. 2.4.

[25] ENISA, Threat Landscape Report 2016 15 Top Cyber-Threats and Trends, January 2016, Ch. 2, accessed 1 September 2017 at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. This product is the fifth in a series of reports analysing cyber-threats.

technical connotation of information that is processed to draw the context is anyhow prevailing.[26]

With regard to Europol, its European Cybercrime Centre (EC3) delivers "cyber-intelligence" to fight cybercrime.[27] This intelligence results from the analysis of information on cybercrime that is gathered by the Centre from a wide array of public and private sources. It is delivered through the following products: (i) the "Cyber Bits", *i.e.* short intelligence notifications on cyber-related topics; (ii) the Open-Source Intelligence (OSINT) Dashboard, which reports the most important cyber-crime related events on weekly base; and (iii) the Common Taxonomy for the National Network of Computer Security Incident Response Teams (CSIRTs).[28] In EC3's perspective, each of these products represents cyber-INT. However, according to the available information, they look more like pieces of knowledge on cybercrime related issues than intelligence. At least this seems to be the case of the Common Taxonomy that is a nomenclature for the classification of cyber incidents or attacks. As per the OSINT Dashboard (therefore not cyber-INT!), it is open source information on the most important events in cybersecurity and cybercrime. With regard to "Cyber Bits", they consists of information on: (i) trends, *i.e.* emerging patterns and new *modi operandi*, tools and techniques that cyber criminals use; (ii) different related aspects of cybercrime such as infrastructure, tools and *modus operandi*; (iii) technical developments that could have an impact on the work of law enforcement authorities, and that can spawn more in-depth reports if it is felt that the initial findings warrant this; (iv) tools that have been developed at the request of a focal point within Europol, a Member State or a European Cybercrime Centre stakeholder.[29] Cyber Bits are generally offered to a large audience even if there are versions of this product that are delivered to law enforcement agencies only. Reasonably, the latter versions should contain more rapidly actionable knowledge, *i.e.* provide operational intelligence that enables short/mid-term actions. However, the actionability of the intelligence delivered through the Cyber Bits should not be over-estimated. As described by Europol, Cyber Bits bring important news to the attention of the law enforcement agencies rather

[26] This makes ENISA ETLs keen on being considered "tactical" cyber-intelligence. See *infra*.
[27] The EC3 was established in 2013 to strengthen the law enforcement response to cybercrime in the EU. Within the EC3 operates the Cyber Intelligence Team (CIT), whose analysts collect and process cybercrime-related information to identify emerging threats and patterns. More info at https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3#fndtn-tabs-0-bottom-1.
[28] *Ibidem*.
[29] *Ibidem*.

than providing them with a detailed assessment.[30] This put in to question their full qualification as intelligence. In general, despite the use of the expression cyber-intelligence by Europol EC3 to qualify its products, it is actually not completely clear what cyber-INT is and how it is crafted.

At the Member States level, the availability of intelligence on cyber-threats is acknowledged as a necessary requirement for engaging in effective prevention of and response to these threats. At least, this emerges from the latest policy instruments adopted and implemented by the British, Dutch, Spanish, Belgian, and Italian Governments to protect their national security and, in particular, improve cybersecurity. To a different extent and by using diverse wording, these instruments promote the mobilisation of relevant resources and capabilities for enhancing the production of intelligence, in particular, cyber-intelligence. This latter expression is formally employed by the Italian National Plan for Cyber-Security.[31] The Plan fosters the "strengthening of cyber-intelligence capabilities" and sustains the development of tools and processes for "the contextual analysis of cyber-events".[32] The definition of cyber-intelligence is provided by the updated version of the *Glossary on Intelligence* published by the Italian Information and Security System.[33] According to the Glossary, cyber-intelligence is the "Research and analysis of relevant information within or regarding the cyberspace in order to prevent, detect, contain and contrast threats to national security, for example, to critical infrastructures.[34] The expression "cyber-intelligence" is also employed by the Belgian Cyber Security Strategy for the defence sector.[35] It is defined as "Activities using all 'intelligence' sources in support of Cyber Security to map out the general cyber threat, to collect cyber intentions and possibilities of potential adversaries, to analyse and communicate, and to identify, locate, and allocate the source of cyber-

---

[30] *Ibidem*.
[31] "Piano Nazionale per la Protezione Cibernetica e Sicurezza Informatica", 2017, accessed 1 September 2017 at http://www.governo.it/sites/governo.it/files/piano-nazionale-cyber-2017.pdf.
[32] *Ibidem*, Indirizzo operativo 1, par 1.2.
[33] Sistema di Informazione per la Sicurezza della Repubblica, "Glossario Intelligence", December 2013, accessed 1 September 2017 at https://www.sicurezzanazionale.gov.it/sisr.nsf/quaderni-di-intelligence/glossario-intelligence.html.
[34] *Ibidem*. In Italian: "Ricerca ed elaborazione di notizie di interesse nel e sul cyber-space al fine di prevenire, rilevare, contenere e contrastare le minacce alla sicurezza nazionale, con riguardo ad esempio alle infrastrutture critiche".
[35] Belgian "Cyber Security Strategy for Defence" (English version), par. 8 accessed 1 September 2017 at https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf.

attacks.[36] No explicit mention of "cyber-intelligence" is given by the UK, Dutch and Spanish cyber-security strategies. With regard to the former, it encourages domestic intelligence and other security/law enforcement agencies to "expand their efforts to identify, anticipate and disrupt hostile cyber activities by foreign actors, cyber criminals and terrorists". According to the strategy "this will improve their intelligence collection and exploitation, with the aim of obtaining *pre-emptive intelligence on the intent and capabilities of our adversaries*" (emphasis added).[37] The Dutch strategy promotes the "Strengthening [*of*] research and analysis capabilities to gain more *insight into threats and risks in the digital domain*", while the Spanish expresses the Government's commitment to "enhance the national capabilities to detect and analyse cyber threats in order to generate the necessary *intelligence for a more effective defence and protection* of national networks (emphasis added).[38] Regardless of the used terminology, these latter reported passages insist on the production of actionable insight into threat actors' "intent and capabilities" or "threat and risks in the digital domain". Such insight should allow its consumers to adopt prevention (pre-empt and anticipate) and effective protection measures. Although not labelled as cyber-intelligence, it seems anyhow evident the reference to the acquisition of a more qualified knowledge than the one provided through narrow-scoped CTI.

Stronger than elsewhere is the push toward the employment of cyber-intelligence-led concepts and solutions that comes from the private sector. Several cyber-security vendors worldwide develop and offer tools and services to enhance their costumers' capabilities to identify and assess

---

[36] *Ibidem*, p. 18.

[37] The UK National Cyber Security Strategy 2016-2021, par. 4.16, 5.0.2, 6.2.5 accessed 1 September 2016 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. Cf. also "The National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom", par. 4.107 and 4.114 accessed 1 September 2017 at https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015, stating that the Government will invest in capabilities to detect and analyse cyber threats, pre-empt attacks and track down those responsible. Furthermore, a new intelligence unit dedicated to tackling the criminal use of the "dark web" is established.

[38] The Dutch "National Cyber Security Strategy 2. From awareness to capability" (English version), Annex I, Objective 1, Action No. 1, accessed 1 September 2017 at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf. See also the Spanish "Estrategia de Ciberseguridad Nacional 2013", p. 31, accessed 1 September 2017 at http://www.lamoncloa.gob.es/documents/20131332estrategiaciberseguridadx.pdf.

potential cyber-threats to their assets.[39] Their proposed tools are often highly-technological. They combine artificial intelligence, machine learning, data analytics and other technologies to generate intelligence for cyber-threats prevention/response.[40] In general, vendors make clear that what they offer are not tradecrafts for the delivery of "technical feeds" on the menaces; they are instruments that produce intelligence through the collection, analysis and contextualisation of relevant threats.[41] Among other things, such an intelligence is premised upon the assessment of an organisation's activities and how they may prompt attacks, the understanding of the motivations and beliefs of a potential threat actor, the analysis of how a geopolitical event may trigger the use of a new attack type. In sum, it is based on the gathering and processing of not only technical data but broader contextual information.[42]

In light of what was described so far, it seems evident that different types of organisations across Europe endorse the idea of employing intelligence to prevent and counter cyber-threats. Sometimes called "cyber-intelligence" while other times not-labelled as such or not-comprehensively described, this knowledge should be crafted through the collection and analysis of information that is not confined to data on network operations and activities but covers broader aspects and implications of cyber-threats. Having said that, one may still wonder what cyber-intelligence more exactly is, and what its production implies. This would require a deeper investigation on the above described initiatives and examination of their adopted concepts and practices. It would also require to look at the intellectual/analytical work that has been carried out on the topic so far. The latter will the object of the following paragraphs.

Cyber-Intelligence: Looking for a Common Understanding

On Terminology and (shared) Definition

[39] The are several companies that provide these tools and services across the globe and Europe. Mapping them is beyond the scope of this paper. A collection of information about companies established in Europe will be included in the research project.

[40] See, *e.g.*, http://www.cyberintelligencecentre.com/.

[41] See *e.g.*: https://www.accenture.com/be-en/insight-accenture-cyber-intelligence-platform; https://www.microsoft.com/en-us/security/intelligence; https://dreamlab.net/en/services/cyber-intelligence/; http://www.silobreaker.com/; http://cscss.org/CIDC/, https://www.blackcube.com/cyber-intelligence/.

[42] Kristofer Månsson, "Why cyber should not be limited to cyber, in Business Reporter", May 2015, accessed 1 September at https://business-reporter.co.uk/2015/05/31/why-cyber-should-not-be-limited-to-cyber/. According to the author says "Cyber-events don't happen in a vacuum. There is context around them that often is hard to see".

In everyday language, "cyber-intelligence" (or whatever it is referred to) is mainly used as an enveloping and catch-all expression. A clearer picture of cyber-intelligence can be obtained by deconstructing the main conceptual elements that are involved in the initiatives that were described above, especially those that provide a definition of cyber-INT. However, this is not enough to understand what "cyber-intelligence" more exactly is. As a product and a process, is it intelligence "from", "on", "within" or "for" the cyberspace or some combination? To what extent does it focus on this space or cover events also occurring in the physical domain? What are the main sources of cyber-INT? How is it crafted? Is the "traditional" intelligence cycle applicable to cyber-intelligence? What are the implications in crafting and sharing cyber-intelligence? Answering to these framework – or other more specific – questions is not trivial.

For instance, the lack of a uniform understanding of the term "cyber" hinders any attempt to come up with a comprehensive and uniform notion of cyber-intelligence. Indeed, whereas it is more or less undisputed establishing what intelligence (as product and process) is, defining it in relation to the cyber domain is challenging.[43] In general, reflections on cyber-intelligence employ concepts, frameworks and terminology derived from the intelligence community and adopt/adapt them to the cyberspace.[44] This seems to be a logical approach given that some concepts are already established and there is no need to "re-invent the wheel". However, one may wonder to what extent these concepts are amenable to be applied to, and function for, a domain that differs from the traditionally known domains. The cyber is in fact a man-made, highly-evolving, technologically-shaped and not-fully tangible environment which, perhaps, needs to be interpreted by using different paradigms.[45] Its interaction with the physical domains are yet to be fully understood. Furthermore, cyber-intelligence is a relatively new practice which is far from being fully tested, assessed, and developed. There is not enough shared

[43] There are different definition of intelligence. Broadly speaking, intelligence is what is produced when collected information is analysed and evaluated. It is both a product and a process. It consists in the gathering, analysis, and the establishment of informed, targeted and actionable knowledge of the present, enabling accurate prediction of the future. It is worth stressing that such knowledge should be 'capable of being acted on or affording ground for an action'. Actionable knowledge is forward-looking. At its core, it is concerned with the possible future, with informed – indeed wise – estimates of future events.

[44] Robert M. Lee, "An Introduction to Cyber-intelligence", 2014, accessed 1 September 2017 at https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/; Stephanie Helm, "Intelligence, Cyberspace and National Security", EMC Chair Conference paper, accessed 1 September 2017 at https://www.usnwc.edu/Academics/Faculty/Derek-Reveron/Workshops/Intelligence,-National-Security-and-War.aspx.

[45] This discussion, although very interesting, falls beyond the scope of this paper.

experience on how it works and on the best capabilities required to carry it out effectively. This hampers any attempt to come up with a thorough interpretative model for cyber-INT.

Having the above in mind is important for adopting a less biased and agnostic approach to cyber-intelligence and to the study of the topic. It helps in understanding why there is not yet an agreed and crystallised definition of cyber-intelligence. Actually, one may wonder whether it is really necessary or desirable to adopt a shared definition of cyber-INT. In principle, a definition can help relevant stakeholders to be consistent when they launch programmes or take actions on cyber-intelligence. It becomes a prerequisite when these stakeholders aim at establishing cooperation mechanisms in the field. This latter aspect is quite important. Indeed, the crafting process of cyber-intelligence requires (ideally) mutual collaboration and knowledge sharing.[46] To be effective and not fragmented, cooperation should be at least premised upon a common language and understanding of the conceptual components of cyber-intelligence and its crafting process.

Cyber-Intelligence: Actionable Knowledge "From", "Through", or "For" the Cyber?

According to the available sources, the study of cyber-intelligence dates back to 2010 when the US based Intelligence and National Security Alliance (INSA) established a Cyber Intelligence Task Force that published a first paper on the topic.[47] The paper set the framework to look at the cyber-domain through an intelligence-led perspective. It also presented the foundational thinking and approach to cyber-intelligence.[48] Since then, other analytical work has been carried out by the same organisation as well as other entities, experts and the academia.[49] The most part of this work pays attention to the notion of cyber-intelligence, the discussion on how this product is crafted, and functions at the strategic, tactical and operational levels within an organization. Military defence, national security, intelligence and cybersecurity are the fields of study within which relevant works are framed.

Basically, the literature describes cyber-intelligence as (the process consisting of and the product resulting from) the collection and analysis of

---

[46] See also *infra*.
[47] INSA is an organisation that facilitates dialogue and collaboration between the public, private, and academic sectors of the US intelligence and national security communities.
[48] INSA, Cyber Intelligence: Setting the landscape for an emerging discipline, 2011, pp. 1 – 20, accessed 1 September 2017 at https://www.insaonline.org/cyber-intelligence-setting-the-landscape-for-an-emerging-discipline/.
[49] See *infra* the footnotes.

information to support decision making on cyber-threats. Depending on the scope of the information gathering activities, the means employed to carry them out, and the final purpose they serve, there are actually two ways to look at/interpret cyber-intelligence.[50]

One way is to think about cyber-INT as intelligence "from" the cyber, *i.e.* knowledge produced through the analysis of any valuable information collected "within" or "through" the cyberspace. This is cyber-intelligence "stricto sensu". From this perspective, "cyber-" refers to both the domain where data are sourced or, in other, words, that vast digital repository of information amenable to be retrieved and processed; and the tools/ techniques/media through which these data are collected (*e.g.* via Computer Network Exploitation technologies and techniques).[51] According to this interpretation, cyber-INT can in principle support decision making in any domain and not only to counter cyber-threats. It can support a broad variety of missions in government, industry, the academia including policy-making, strategic planning, international negotiations, risk management, strategic communication in further areas than cyber-security. In other words, cyber-intelligence may operate "independently and does not necessarily need to support a cybersecurity mission".[52] However, given that cyber-intelligence is often discussed in relation to cybersecurity or to the prevention of and response to cyber-threats, these are the primary – but, again, not exclusive – goals of this kind of intelligence.

Another way to interpret cyber-INT is considering it as intelligence "for" the cyber, *i.e.* insight that stems out from an all-source intelligence activity occurring within and outside the cyberspace. It is cyber-intelligence "lato sensu". In this sense, the intelligence "for" the cyber can also include (or be built on) intelligence "from" the cyber. It can draw from any intelligence discipline that supplies crucial knowledge, regardless of the source, method, or medium employed for crafting it. As such, cyber-intelligence may therefore result from the combination of Open Source Intelligence (OSINT), Signal Intelligence (SIGINT), Geospatial Intelligence (GEOINT), Social Media

---

[50] Matthew M. Hurley, "For and from Cyberspace Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance" *Air & Space Power Journal*, Vol 26, No. 6 (2012), pp. 12-33.

[51] Ross W. Bellaby "Justifying Cyber-intelligence?", *Journal of Military Ethics*, Vol. 15, No. 4, (2016), pp. 299-319; Matthew M. Hurley, cit., p. 13. Computer Network Exploitation or cyber exploitation refers to the secret collection and reproduction of digital data from computers or networks.

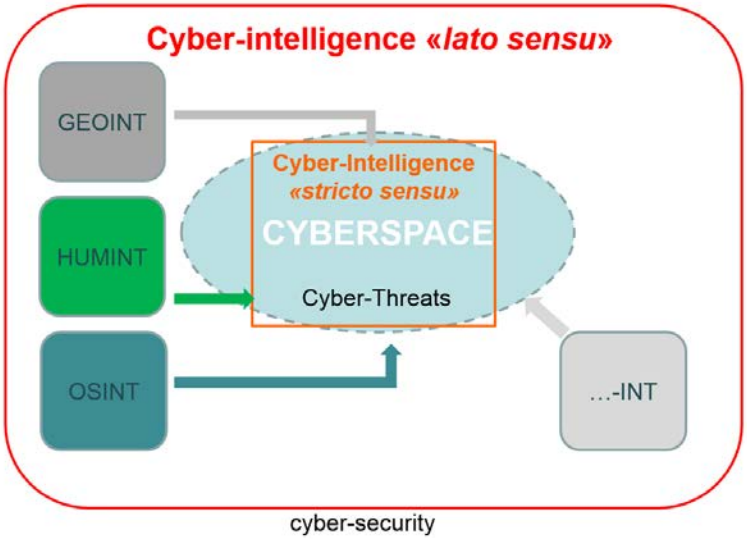
[52] Troy Townsend, Melissa K. Ludwick, Jay McAllister, Andrew O. Mellinger, Kate A. Sereno, "Cyber Intelligence Tradecraft Project: Summary of Key Findings", the Software Engineering Institute (SEI) Emerging Technology Center at Carnegie Mellon University, September 2013, pp. 2.01-2.20, spec. 2.5 at http://www.sei.cmu.edu/about/organization/etc/citp-summary.cfm. The full report is available at http://www.sei.cmu.edu/about/organization/etc/citp.cfm.

Intelligence (SOCMINT), and Human Intelligence (HUMINT).[53] From this point of view, cyber-intelligence is less a discipline itself than an analytic practice relying on information/intelligence collected also through other disciplines and that is intended to inform decision makers on issues pertaining to activities in the cyber domain.[54] What qualifies this kind of intelligence as "cyber-" is the purpose for which it is crafted: support decision making on cyberspace related issues.

The two discussed perspectives on cyber-intelligence – intelligence "from" and "for" the cyber – are often condensed in to one single comprehensive concept (Figure 1). This is also due to the fact that intelligence "for" the cyber actually incorporates the one "from" the cyber. The result is a broader notion of cyber intelligence that includes the collection, processing, evaluation, analysis, integration, and interpretation of information that is available "within", "though" and/or "outside" the cyberspace to enhance decision-making on cyber-related menaces. The described notion of cyber intelligence seems to correspond to the one endorsed by the Belgian Strategy for Cyber-Security for the Defence and the Italian Cyber Security Strategy (*cf.* the Glossary).[55]

Figure 1. Cyber-intelligence "stricto sensu" and "lato sensu"

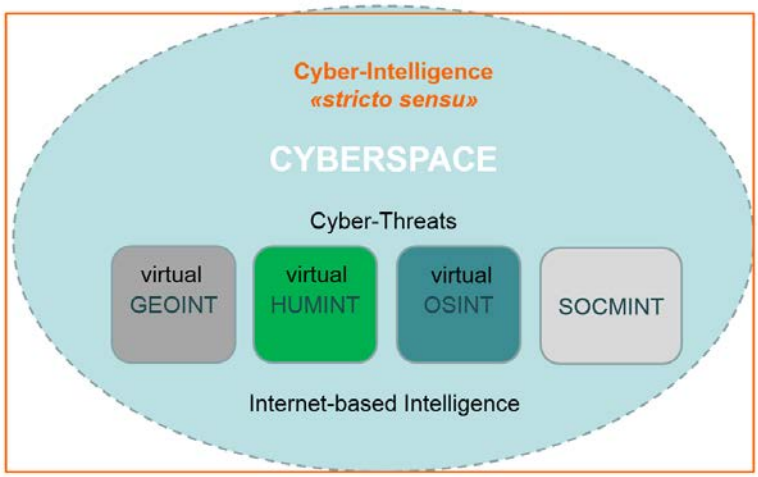
[53] Aaron F. Brantly, *The Decision to attack. Military and Intelligence Cyber-Decision Making*, (Athens GA: The University of Georgia Press, 2016), Ch. 7, pp. 103-108 and 116-121.
[54] INSA, Operational Levels of Cyber Intelligence, September 2013, pp. 1-14, accessed 1 September 2017 at https://www.insaonline.org/operational-levels-of-cyber-intelligence/. On the existing intelligence disciplines, see among others The UK MoD, "Joint doctrine publication 2-00, understanding and intelligence support to joint operations", JDP 2-00, 2011, accessed 1 September 2017 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf. In Italian: Glossario intelligence, cit.
[55] See *supra*.



However, it is worth noting that when looking at the "traditional"-INT disciplines encompassed by the notion of cyber-intelligence "lato sensu", their narrower and circumscribed projection to the cyberspace has determined the development of *ad hoc* concepts and approaches (or simply reference to expressions) like: virtual HUMINT, virtual or internet-based OSINT, virtual COMINT, etc (Figure 2). The adjective "virtual" indicates that intelligence activities are carried out within the cyberspace or through computer-generated tools (intelligence "stricto sensu"). Its association with "traditional" –INT concepts/ practices is made for referring to the adoption of methods/approaches/tools that are employed by these practices and adapted for the cyberspace.[56] A bit different from the above concepts is the notion of social media intelligence (SOCMINT) which is considered by some scholars/practitioners as having proper features that can be difficulty linked to other intelligence disciplines.[57]

Figure 2. Virtual -INTs

[56] For example, the virtual HUMINT approach aims at collecting tactical/operational intelligence from the information generated by members of virtual communities. Practically, it consists in establishing and operating a virtual identity (avatar) to gain trust from, and create long-term relationships with, the members of the participated/monitored communities, as well as recruit, handle, manipulate and decept them with the purpose of collecting information. As evident, it adopts and relies on HUMINT traditional approaches but apply and adapt them to the cyberspace. One may wonder to what extent it is possible to consider virtual HUMINT a specific sub-category of HUMINT or think about it as an emerging practice. Answering to this question would require examining in more details the differences and similarities between these activities and the functions they consist of. However, this is far beyond the scope of the present paper.
[57] Omand et al., "#Intelligence". Cf. Bonfanti, "Social media intelligence", 231-262.



With regard to the information to be retrieved, this may range from network technical data (*e.g.* hardware and software data), data on hostile organizations and their capabilities, ongoing cyber activities, to potentially any relevant geopolitical event.[58] The type of data as well as their classification are not functional to the definition of cyber-intelligence. Data can be raw or already processed information; they can be obtained – legally or through unlawful intrusion/exploitation actions – from open, proprietary, or other classified sources.[59] Actually, as the literature suggests, multiple sources of information are needed to develop a more holistic understanding of the threat environment and producing comprehensive cyber-INT.[60] The most important aspect of the data is that they should be (somehow) validated.[61] When analysed, information should allow decision makers to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of action.[62] This is the main feature of cyber-intelligence, *i.e.* its enabling goal: to provide its consumers with insight into potentially hostile activities that may

[58] Jung-ho Eom, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace" *International Journal of Software Engineering and Its Applications* Vol. 8, No. 9, 2014, pp.137-146. The article deals with cyber- intelligence for military purposes.
[59] Robert M. Lee, "Cyber Intelligence Collection Operations", 2014, accessed 1 September 2017 at https://www.tripwire.com/state-of-security/security-data-protection/cyber-intelligence-collection-operations/.
[60] INSA, cit., p. 1.
[61] Validation is often a challenging task due to the high volatility, anonymity and uncertainty of data and heterogeneity of data sources.
[62] Troy Townsend, Melissa K. Ludwick, cit.

occur in the cyber domain or be perpetrated through the cyberspace, and allow them to design effective preventative (proactive) or counteractive (reactive) measures.

Depending on its scope or level of actionability, cyber-intelligence can be strategic, tactical or operational.[63] There is actually no uniform interpretation of what the different levels of cyber-INT should consist in. According to the large part of the available literature, strategic cyber-INT focuses on the long-term, typically reviews trends in current and emerging threats, as well as examines opportunities to contain these threats. It serves apical decision making processes aimed at the achievement of an organization's mission, the determination of its direction and objectives. It covers the threat landscape for macro trends (*e.g.* political, social, economic) affecting the organization and identifies who are the threat actors, what are their goals, why, and how they will likely attempt to achieve them. It is rich in contextual information.[64] Tactical cyber-intelligence concerns what is happening on the network. It also examines the strength and vulnerabilities of an organisation, and the tactics, techniques and procedures (TTPs) employed by threat actors.[65] Due to its nature and reach, tactical cyber-INT corresponds to what is generally meant as cyber-threat intelligence.[66] Generally more technical in nature, it informs the specific network-centred steps and actions the organization takes to protect assets, maintain continuity, and restore operations. As far as operational cyber-INT is concerned, it consists into knowledge on imminent or direct threats to an organisation. It enables and sustain day-to-day operations and output. At this level, cyber-intelligence looks at the organization's internal processes and vulnerabilities.[67]

---

[63] The INSA defines each operational level of cyber intelligence according to: (i) the nature, role and identity of the consumer; (ii) the decisions the consumer will make; (iii) the timeframe in which the consumer tends to operate; (iv) the scope of collection; (v) the characterization of potential adversaries; and (vi) the level of technical aptitude required for cyber intelligence collection. See references in the next footnotes. *Cf.* also Randy Borum, "Getting Left of the hack. Honing Your Cyber Intelligence Can Thwart Intruders", September 2014, accessed 1 September 2017 at https://works.bepress.com/randy_borum/63/; INSA, cit., pp. 7 ff.

[64] Randy Borum, John Felker, Sean Kern, Kristen Dennesen, Tonya Feyes, "Strategic Cyber Intelligence" *Information & Computer Security*, Vol. 23, No. 3, 2015, pp. 317-332. See also, INSA, Strategic Cyber intelligence, 2014, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/strategic-cyber-intelligence/.

[65] INSA, Tactical Cyber Intelligence, 2015, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/tactical-cyber-intelligence/.

[66] See *supra*.

[67] INSA, Operational Cyber Intelligence, 2015, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/operational-cyber-intelligence/.

It worth repeating that the described distinction between the levels of cyber-INT is mainly scholastic. In practice, there is no clear demarcation from one level of intelligence to another; they frequently overlap or are combined. Furthermore, the meaning of strategic, tactical, and operational is likely to vary across organizations because of their size, complexity, mission and related attributes.[68] Regardless of any clear-cut demarcation among the levels, quite important is the capacity of an organisation to consider all these levels and craft intelligence that allows it to understand the challenges and opportunities it is likely to encounter in the short-mid-long terms. As a finished product, it seems there are no established formats or standards for presenting cyber-intelligence to decision-makers.

What has been discussed so far helps in drawing a clearer picture of cyber-intelligence and identifying the main conceptual components involved in its notion – at least the one identified by the literature? Further comprehension of cyber-INT can be obtained through the discussion of how this product is crafted. Such a discussion requires the examination of those set of (sequential?) operations resulting in cyber-INT and the required capabilities (human, organisational and technological) to carry them out.

The Cyber-Intelligence Process: Alternative *vs* Traditional Models

Just like the case of other intelligence products/disciplines, cyber-intelligence is crafted through a set of activities/functions (that has collection and analysis at its core). Traditionally, this set of functions is represented and explained through the "intelligence cycle" model.[69] The model has been studied and questioned several times by practitioners and academics to the point that alternative models were proposed and discussed.[70] The "validity/applicability" of the traditional intelligence cycle model is also questioned as far as cyber-intelligence is concerned. As it is argued, the traditional model has a limited applicability to the cyber and cannot accurately explain the crafting process of cyber-intelligence. Meant as a linear and reiterative cycle, it does not emphasize the inter-related nature of the

---

[68] INSA, Strategic Cyber intelligence, cit. p. 4.

[69] While there are different representations of the Intelligence cycle, the most common comprises five distinct phases: Planning and Direction, Collection; Processing, Analysis, and Dissemination. The logic of the intelligence cycle lies in the assumption that consumers of the finished intelligence make decisions on the basis of this product, and these decisions may lead to the levying of more requirements, thus triggering the cycle again. On the intelligence cycle see Mark Phythian (Ed.), *Understanding the Intelligence Cycle* (London and New York: Routledge 2013).

[70] *Ibidem*.

activities (planning, collection, processing etc.) the cyber-intelligence process consists of, and their mutual relevance. In other words, it does not capture their inter-dependencies and mutual influences.

In light of the above, an alternative model is proposed to explain the cyber-intelligence process.[71] It differs from the traditional intelligence cycle for the adopted terminology, the non-linear and strictly consequential logic of the functions the process consists of, the decomposition of the analysis function in to two specialised functions (the technical or functional analysis and the strategic analysis), and the capacity to capture both the "narrow" technical cybersecurity and "wider" cyber-threats prevention purposes that cyber-intelligence can serve within an organisation. As it is represented, the proposed model accommodates the interpretation of cyber-intelligence as an analytic practice relying on information/intelligence collected also through other disciplines and which is intended to inform decision-makers on issues pertaining to activities in the cyber domain.[72]

The proposed model consists of five functions: (i) the determination of the "Environment" which establishes the scope of the cyber intelligence effort and influences what information is needed to accomplish it;[73] (ii) the "Data Gathering" *i.e.* the exploration of data sources and collection-filtering of information through automated and labour-intensive tools;[74] (iii) the "Functional Analysis", *i.e.* the performance of technical and tailored analysis (typically in support of a cybersecurity mission) that is aimed at deriving the

---

[71] Troy Townsend, Melissa K. Ludwick, *et alii*, cit.

[72] *See supra*.

[73] Troy Townsend, Melissa K. Ludwick, *et alii,* p. 2.9. Environment is meant as both internal and external. The determination of the internal environment includes the studying of an organisation's global cyber presence, the infrastructure that are accessible through the Internet, as well as the definition of what data needs to be collected to maintain network situational awareness. Externally, the determination of the environment requires to know which the entities capable of affecting organizations' networks are. It requires to find out and map system vulnerabilities, intrusion or network attack vectors, and the tactics, techniques, procedures, and tools used by relevant threat actors. As it is suggested: "By investing the time and energy to define the environment, organizations significantly improved their data gathering efforts, resulting in more efficient and effective cyber intelligence programs".

[74] *Ibidem*, p. 2.11. Data gathering should cover both internal (*e.g.,* net-flow, logs, user demographics) and external sources (*e.g.,* third-party intelligence providers, open source news, social media). It should focus on the pertinent threats and strategic needs as identified while learning about their organization's environment. Indeed, to be effective data gathering should be based on the definition of the environment. It should target the necessary data for conducting meaningful analysis on critical cyber threats.

"what" and "how" of cyber threats;[75] (iv) the "Strategic Analysis" entailing the review, integration with contextual information, and further elaboration of the functional cyber-intelligence with the goal of answering the "who" and "why" questions;[76] and (v) the decision maker "Reporting and Feedback", *i.e* dissemination of cyber-intelligence to decision makers and collection of feedback.[77]

The main dependencies and mutual influences among the described functions are the following. Data gathering should be premised upon the determination of the environment which is itself influenced by the decisions taken by the organisation on the basis of consumed cyber-intelligence. The intelligence resulting from the functional analysis can inform decisions on actions to be taken on the technical-network level of an organisation which, in turn, impact on the determination of the internal environment; the same goes with intelligence resulting from the strategic function which impact on both the internal and external environment. The strategic function also renders the intelligence resulting from the functional analysis more consumable by apical decision makers who may not have a technical background. From this perspective, it is a sort of add-on application who contributes in bridging the communication gap between analysts and top decision makers. These latter provide their feedback on the received intelligence to shape analytical functions, adjust the direction of the organisation and therefore influence the environment.

Questioning the "validity" of the discussed cyber-intelligence process model is beyond the scope of this paper. However, there are few considerations that are worthy of being made. First of all, the proposed model has been designed following an empirical work which mapped and assessed current practices in cyber-intelligence in the US. It is grounded on data and represents what the state of the art within selected organisations. It has also a normative reach *i.e.* suggests how the process should work to be effective. Furthermore, the proposed model has the advantage to be relatively simple while, at the same time, representative of practices adopted by different types of organisations *e.g.* small corporations, larger industries, and governmental

---

[75] This function includes the verification/validation of data based on the quality of the source, reporting history and independent verification of corroborating sources. *Ibidem*, p. 2.13.
[76] *Ibidem*, 2.15. Strategic analysis adds perspective, context, and depth to functional analysis. It is ultimately rooted in technical data, but incorporated information outside traditional technical feeds. The resulting strategic analysis populated threat actor profiles, provided global situational awareness, and informed decision makers of the strategic implications cyber threats posed to organizations, industries, economies, and countries.
[77] *Ibidem*, p. 2.17.

agencies. However, its representativeness is likely to fade away at both the lower and higher levels of occurrence of the cyber-intelligence process *i.e.* at the individual and multi-partnership or transnational levels. Especially at the latter level, the degree of organisational/institutional complexity will probably render the intelligence model unfitted. In addition, technological developments that are likely to occur in the field of cyber will probably impact on the model and require further re-elaborations.[78] Lastly, the proposed model still suggests that collection and analysis are sequential *i.e.* the latter can only begin once the former is complete. In practice, the two functions are interactive and occur concurrently. The above said, the described model represents a sound attempt to better explain how cyber-intelligence is (should be) crafted.[79]

The Most Wanted: Skilled Analysts and Advanced Analytics

As one may understand, producing valuable cyber-intelligence requires an organisation to acquire significant capabilities in terms of human, technical, organisational, and financial resources. It also requires the adoption of tailored and effective procedures.[80]

As far as the human resources are concerned, the cyber-intelligence crafting process should rely on skilled individuals to perform the collection and the analysis of information as well as the communication of the resulting intelligence to decision-makers. On top of the characteristics (traits and competences) any intelligence practitioner should possess (*e.g*. understanding the intelligence requirements, defining a problem, apply research and analysis methods and think strategically to suggest a course of action), the cyber-intelligence operator should combine a mix of technological and human and social science culture/skills.[81] This is required by the nature of cyber-intelligence that demands analysts to deal with technical data on information systems, networks and tools, as well as broad contextual information of

[78] This is actually acknowledged by the promoters of this model when discussing about analytical capabilities. "Because technology changes so quickly, the process of producing cyber intelligence analysis had to be dynamic enough to capture rapidly evolving tools, capabilities, and sophistication of adversaries".

[79] A deeper discussion of the cyber-intelligence process as well as the formulation on another alternative interpretative model will be carried out within the research project.

[80] Needless to say this hold also true with regard to other intelligence practices.

[81] Melissa K. Ludwick, Troy Townsend, Joan P. Downing, "White Paper – CITP Training and Education", Sep 2013, 6.1-6.24, accessed 1 September 2017 at http://www.sei.cmu.edu/about/organization/etc/upload/whitepaper.pdf.

different typology. The operator's knowledge should in principle span from operating systems and scripting and coding techniques, to geopolitics, terrorism, and organised crime. Since it is most unlikely that one person possesses such a broad and overarching knowledge, what cyber-INT operators should principally have is the aptitude to be collaborative and keen on working in multidisciplinary teams – within which sectorial competencies can be combined.

To a significant extent, collection and analysis can be automatized through the employment of advanced technologies.[82] These can assist cyber-intelligence practitioners to search and retrieve data and make sense of them. Regardless of any specific feature of the employed technological solutions, it worth stressing that these are to be meant as tools that assist practitioners with performing cyber-INT and speed-up data processing and analysis. They do not carry out all the cyber-INT process' functions and deliver ready-to-be-consumed intelligence. Furthermore, given the nature of cyber-INT, analytics should be able to perform processing, correlation, integration, visualisation of large sets of data that have different format and stem from diverse sources which are explored through various intelligence disciplines.[83] Even if capable to do that in an effective manner, the process will anyhow benefit from the practitioner' personal traits, competencies and experience. In conclusion, although amenable to be executed with the extensive support of technological tools, cyber-intelligence as a process requires – and cannot get rid of – human operators (and their human brain!).

Crafting and Sharing: Two Faces of the Same Coin

Another aspect concerning the crafting of comprehensive cyber-intelligence is the need to have access to multiple sources of information or knowledge. This is often not possible for a single organisation who therefore needs to be provided with data, or even finished intelligence, by external entities. Regardless of the basis (voluntary or mandatory) upon which the provision of data and knowledge takes place, this should in principle occur regularly and be framed within a (formal or informal) cooperation mechanism which has information sharing as object.[84] Indeed, the crafting of cyber-intelligence can significantly benefit from the integration and analysis of

---

[82] *Cf.* also *supra*.
[83] *Cf.* also *supra.*
[84] AFCEA International Cyber Committee, "Cyber Intelligence Sharing", 2014, accessed 1 September 2017 at https://www.afcea.org/committees/cyber/documents/AFCEACyberIntelligenceSharingPaper-FinalVersionforPublication_002.pdf.

information or further intelligence that are dispersed across sources accessible by third parties only (*e.g.* governmental agencies, private organisations, academia) and then shared.

Same as for other -INT disciplines, the production and the sharing of cyber-intelligence are interrelated processes.[85] They are actually more interrelated than it would seem at the first sight. Indeed, cooperation among cyber-intelligence stakeholders – at both the domestic and international level – may contribute to crafting more valuable intelligence, *e.g.* making accurate, complete and corroborated threat assessments and predictions. Having multiple actors – each of them with specific remit and capabilities in information and intelligence gathering – that combine the knowledge they have respectively acquired may result in "enhanced" cyber-intelligence products to be consumed for designing more effective preventive and counter-measures. Put differently, the enhanced cyber-intelligence products that may result from improved information sharing could provide more sound intelligence support to face cyber-threats; and the more this support proves to be sound and actionable, the more – in principle – relevant stakeholders are likely to incentivise the sharing of cyber-intelligence.

The above argument seems to work well in principle. The reality sounds different: organisations tend to limit their engagement in information or intelligence sharing. Differently from the case of "general" intelligence cooperation, the production and sharing of cyber-intelligence face further hurdles. These latter have been already documented with regard to the exchange of "information" – not intelligence – in the context of network and information security.[86] The same goes with the limits to the sharing of "cyber-threat intelligence".[87] Some of the identified hurdles are attributed to significant involvement of private actors in the production and sharing of cyber-intelligence. These actors play a central role in the collection of information that is relevant for determining the threats landscape. In general, they are not keen on sharing this information, or exchanging their in-house produced intelligence, for different reasons (reputational risks, protection of sources, unwanted transfer of technological knowledge, and legal liability) among which the general lack of trust of their peers or other involved

---

[85] Matteo E. Bonfanti, cit.

[86] *Cf. e.g.* ENISA & RAND Europe, "Incentives and Challenges to Information Sharing", 2010, accessed 1 September 2017 at https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing.

[87] *Cf. e.g.* CERT-UK, "Integrating Threat Intelligence. Defining an Intelligence Driven Cyber Security Strategy", 2015, at https://www.cert.gov.uk/wp-content/uploads/2015/03/CPNI CONTEXT_CERT-Threat_Intelligence.pdf.

stakeholders – both national and international. In conclusion, poor cyber-intelligence cooperation may result in degraded overall prevention of, and response to, cyber-threats.

Conclusions: Which Way Forward to Establishing Cyber-Intelligence Mechanisms in Europe?

As above discussed, there is a growing push towards the adoption of intelligence-led concepts, approaches and solutions to counter cyber-threats in Europe. This push comes from different representatives of the European cyber-security community. Initiatives in the field have already been promoted by the EU, its Member States and other private organisations. Some of these initiatives address the crafting of "cyber-intelligence" specifically. Although not always defined, cyber-INT is generally meant as the practice that consists in the gathering and analysis of an all-source of information/intelligence to prevent and contrast cyber-threats. Basically, this interpretation corresponds to the notion of cyber-intelligence discussed by the available literature on the topic. The same literature which also explains how cyber-INT is (should be) crafted and identifies the required capabilities for producing it.

Regardless of any manifested intention to go for the adoption of cyber-intelligence concepts or solutions by European or national agencies and organisations, the effective implementation of dedicated programmes in the field requires significant efforts by their promoters. It requires a better understanding of what cyber-INT is and the purposes it can serve, the acknowledgment of the challenges surrounding its crafting process, the identification of the actors that should be involved in the process, and the determination of the resources that are needed to acquire the relevant capabilities. As per the latter, it seems paramount for organisations to invest in the employment of skilled cyber-INT operators or support the run of *ad-hoc* training for internal resources. It is likewise important for them to sustain the development and acquisition of technological tools to be employed for the collection and analysis of information stemming from multiple sources. All this should be combined with the adoption of tailored organisational structures and internal processes. Furthermore, given the above discussed interrelation between the production and the sharing of cyber-intelligence, *ad hoc* cooperation mechanisms to foster the flow of information or finished cyber-intelligence among relevant actors should be established. Cooperation may occur bilaterally or multilaterally. If possible, it should involve the transnational level too. As per the latter, it does not seems that the EU can support the flow of information and intelligence on cyber-threats more than it

presently does within the ENISA and Europol. Given its close ties to Member States' national (cyber-) security (falling within their national sovereignty and domestic jurisdiction), the sharing of cyber-intelligence would require enhanced cooperation among the EU Member States – which is not in place at the moment. However, the EU institutions and their agencies can provide structured platforms for discussion and further negotiations. At the domestic level, cooperation mechanisms should be established within private and public cybersecurity stakeholders. As already pointed out, there are still several obstacles in establishing such cooperation frameworks. However, the growing reach of the menaces coming from the cyberspace and the (yet to be fully) spread awareness of the "need to share" among cyber-intelligence stakeholders would probably induce them to improve their initiative in information/intelligence sharing.

There is a final annotation. The use of the word "practice" rather than "discipline" across this paper is not random. Although the most part of the literature considers cyber-INT being an already-established or soon-to-become-established discipline, it does not seem the case – at least in Europe. The lack of a more mature theoretical elaboration of cyber-INT coupled with the relatively limited experience on it, makes it difficult to consider this type of intelligence a recognised area or branch of intelligence. In other words, cyber-INT should not be considered a discipline because it has not yet been sufficiently defined and practiced. Furthermore, as described above, the nature of cyber-INT and its crafting process makes it less a discipline than an analytic practice which relies on information/intelligence collected also through other disciplines. Of course, nothing prevents cyber-INT to establish itself as a discipline which employs specific technical or human resources throughout the different functions of its crafting process.

References:

1. AFCEA International Cyber Committee, "Cyber Intelligence Sharing", 2014, accessed 1 September 2017 at https://www.afcea.org/committees/cyber/documents/AFCEACyberIntelligenceSharingPaper-FinalVersionforPublication_002.pdf.

2. Barnard-Wills, David, Ashenden, Debi, (2012), "Securing Virtual Space: Cyber War, Cyber Terror, and Risk", *Space and Culture*, Vol. 15, No. 2, 2012, pp. 110-123.

3. Bellaby, Ross W. "Justifying Cyber-intelligence?", *Journal of Military Ethics*, Vol. 15, No. 4, (2016), pp. 299-319; Matthew M. Hurley, cit., p. 13.

4. Bonfanti, Matteo E., (2016), "Collecting and Sharing Intelligence on Foreign Fighters in the EU and its Member States: Existing Tools, Limitations and

Opportunities", in A. de Guttry, C. Paulussen, F. Capone, *Foreign Fighters under International Law and Beyond*, (The Hague: Springer, 2016), pp. 333-353;

5. Borum, Randy, "Getting Left of the hack. Honing Your Cyber Intelligence Can Thwart Intruders", September 2014, accessed 1 September 2017 at https://works.bepress.com/randy_borum/63/; INSA, cit., pp. 7 ff.

6. Borum, Randy, Felker, John, Kern, Sean, Dennesen, Kristen, Feyes, Tonya, "Strategic Cyber Intelligence" *Information & Computer Security*, Vol. 23, No. 3, 2015, pp. 317-332. See also, INSA, Strategic Cyber intelligence, 2014, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/strategic-cyber-intelligence/.

7. Brantly, Aaron F., *The Decision to attack. Military and Intelligence Cyber-Decision Making*, (Athens GA: The University of Georgia Press, 2016), Ch. 7, pp. 103-108 and 116-121.

8. Caligiuri, Mario, (2016), *Cyber Intelligence. Tra libertà e sicurezza* (Roma: Donzelli, 2016), Id., "Cyber intelligence, la sfida dei data scientist", June 2016, accessed 1 September 2017 at https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cyber-intelligence-la-sfida-dei-data-scientist.html,

9. "Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", Brussels, 2016, OJ C 75, 10.3.2017, pp. 124-128, par. 2.2.2.

10. Council of the EU, "EU Cyber Defence Policy Framework, Brussels", 18.11.2014, pp. 7, accessed 1 September 2017 at https://ccdcoe.org/sites/default/files/documents/EU-141118-EUCyberDefencePolicyFrame.pdf.

11. CERT-UK, "Integrating Threat Intelligence. Defining an Intelligence Driven Cyber Security Strategy", 2015, at https://www.cert.gov.uk/wp-content/uploads/2015/03/CPNI_CONTEXT_CERT-Threat_Intelligence.pdf.

12. "Cyber Security Strategy for Defence" (English version), par. 8 accessed 1 September 2017 at https://ccdcoe.org/sites/default/files/strategy/Belgian%20Defence%20Cyber%20Security%20Strategy.pdf.

13. Den Boer, Monica, (2015), "Counter-Terrorism, Security and Intelligence in the EU: Governance Challenges for Collection, Exchange and Analysis" *Intelligence and National Security*, Vol. 30, 2015, pp. 402-419.

14. ENISA, Big Data Threat Landscape and Good Practice Guide, January 2016, accessed 1 September 2017 https://www.enisa.europa.eu/publications/bigdata-threat-landscape.

15. ENISA, Threat Landscape Report 2015, Ch. 2.1; Threat Landscape Report 2014, Ch. 2.4.

16. ENISA, Threat Landscape Report 2016 15 Top Cyber-Threats and Trends, January 2016, Ch. 2, accessed 1 September 2017 at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016. This product is the fifth in a series of reports analysing cyber-threats.

17. ENISA & RAND Europe, "Incentives and Challenges to Information Sharing", 2010, accessed 1 September 2017 at https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing.

18. Eom, Jung-ho, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace" *International Journal of Software Engineering and Its Applications* Vol. 8, No. 9, 2014, pp.137-146.

19. EPSC Strategic Notes, "Building an Effective European Cyber Shield Taking EU Cooperation to the Next Level", Issue 24, 2017, p. 7, accessed 1 September 2017 at https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf.

20. EU Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final, Brussels, 7.2.2013, p. 10 and 17.

21. "Estrategia de Ciberseguridad Nacional 2013", p. 31, accessed 1 September 2017 at http://www.lamoncloa.gob.es/documents/20131332 estrategiaciberseguridadx.pdf

22. Gori, Umberto, Germani, Luigi S., (2011), *Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia* (Bologna: Franco Angeli 2012).

23. Gruszczak, Arthur, (2016), *Intelligence Security in the European Union. Building a Strategic Intelligence Community*, (London: Palgrave-McMillian, 2016).

24. Helm, Stephanie "Intelligence, Cyberspace and National Security", EMC Chair Conference paper, accessed 1 September 2017 at https://www.usnwc.edu/ Academics/Faculty/Derek-Reveron/Workshops/Intelligence,-National-Security-and-War.aspx.

25. Hurley, Matthew M., "For and from Cyberspace Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance" *Air & Space Power Journal*, Vol 26, No. 6 (2012), pp. 12-33.

26. INSA, Cyber Intelligence: Setting the landscape for an emerging discipline, 2011, pp. 1 – 20, accessed

27. INSA, Operational Levels of Cyber Intelligence, September 2013, pp. 1-14, accessed 1 September 2017 at https://www.insaonline.org/operational-levels-of-cyber-intelligence/.

28. INSA, Tactical Cyber Intelligence, 2015, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/tactical-cyber-intelligence/.

29. INSA, Operational Cyber Intelligence, 2015, pp. 1-16 accessed 1 September 2017 at https://www.insaonline.org/operational-cyber-intelligence/.

30. Kime, Brian P., (2017), "Threat Intelligence: Planning and Direction", accessed 1 September 2017 at https://www.sans.org/reading-room/whitepapers/ threats/threat-intelligence-planning-direction-36857.

31. Lee, Robert M., (2014), "An Introduction to Cyber-intelligence", accessed 1 September 2017 at https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber-intelligence/;

32. Lee, Robert M., "Cyber Intelligence Collection Operations", 2014, accessed 1 September 2017 at https://www.tripwire.com/state-of-security/security-data-protection/cyber-intelligence-collection-operations/.

33. Ludwick, Melissa K., Townsend, Troy, Downing, Joan P., "White Paper – CITP Training and Education", Sep 2013, 6.1-6.24, accessed 1 September 2017 at http://www.sei.cmu.edu/about/organization/etc/upload/whitepaper.pdf.

34. Månsson, Kristofer, (2015), "Why cyber should not be limited to cyber, in Business Reporter", May 2015, accessed 1 September at https://business-reporter.co.uk/2015/05/31/why-cyber-should-not-be-limited-to-cyber/.

35. Montecillo, Michael, (2014), "Why Context is King for Enterprise IT Security", April 2014 accessed 1 September 2017 at https://securityintelligence.com/enterprise-it-security-context-king/.

36. "National Cyber Security Strategy 2. From awareness to capability" (English version), Annex I, Objective 1, Action No. 1, accessed 1 September 2017 at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS2Engelseversie.pdf.

37. Office of the Director of National Intelligence, "The National Intelligence Strategy of the United States of America", 2014, pp. 1-24, accessed 1 September 2017 at https://www.dni.gov/files/2014_NIS_Publication.pdf.

38. Phythian, Mark (Ed.), *Understanding the Intelligence Cycle* (London and New York: Routledge 2013).

39. Regulation (EU) 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, Strasbourg, in OJ L 165/41, 18.6.2013, pp. 41-58.

40. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, Strasbourg, in OJ L 135, 24.5.2016, p. 53-114.

41. Sistema di Informazione per la Sicurezza della Repubblica, "Glossario Intelligence", December 2013, accessed 1 September 2017 at https://www.sicurezzanazionale.gov.it/sisr.nsf/quaderni-di-intelligence/glossario-intelligence.html.

42. UK MoD, "Joint doctrine publication 2-00, understanding and intelligence support to joint operations", JDP 2-00, 2011, accessed 1 September 2017 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

43. US Department of Defense Science Board, "Resilient military systems and the advanced cyber threat", January 2013, pp. 46 and 49, accessed 1 September 2017 at http://www.dtic.mil/docs/citations/ADA569975.

44. US Department of Defense Science Board, "The Department of Defence Cyber Strategy", April 2015, p. 24 accessed 1 September 2017 at https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

45. Teti, Antonio, (2013), "Cyber Intelligence e Cyber Espionage. Come Cambiano i Servizi di Intelligence nell'era del Cyber Spazio" *Gnosis. Rivista Italiana d'Intelligence*, Vol. 3, 2013 pp. 95-121;

46. The UK National Cyber Security Strategy 2016-2021, par. 4.16, 5.0.2, 6.2.5 accessed 1 September 2016 at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

47. "The National Security Strategy and Strategic Defence and Security Review 2015. A Secure and Prosperous United Kingdom", par. 4.107 and 4.114 accessed 1 September 2017 at https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015,

48. Townsend, Troy, Ludwick, , McAllister, Jay, Mellinger, Andrew O., Sereno, Kate A., "Cyber Intelligence Tradecraft Project: Summary of Key Findings", the Software Engineering Institute (SEI) Emerging Technology Centre at Carnegie Mellon University, September 2013, pp. 2.01-2.20, spec. 2.5 at http://www.sei.cmu.edu/about/organization/etc/citp-summary.cfm. The full report is available at http://www.sei.cmu.edu/about/organization/etc/citp.cfm.