Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice

Matteo E. Bonfanti

Similar to other cyber-related notions, there is not any crystallized definition of "cyber intelligence," nor are there enough studies focusing on how it is crafted. In light of the above, the present paper draws a clearer picture of this emerging practice by taking stock of the existing analytical work on the topic. The paper reviews the available scientific literature addressing cyber intelligence, discusses the notion of cyber INT, and examines how this intelligence is crafted through the lens of the (cyber) "intelligence cycle." The paper concludes by stressing the importance of developing a clear and shared understanding of cyber intelligence among relevant security and, especially, cybersecurity stakeholders.

Keywords: Cybersecurity, intelligence, cyber intelligence, cyber intelligence process, notion, models

Introduction

Over the last decade, there has been a growing push toward adopting intelligence-led approaches/solutions to deal with cyber threats. The push has come from several members of the (not-formalized) international cybersecurity community that consists of representatives from supranational institutions and agencies, domestic public bodies, private organizations, and academia. They have, for instance, sponsored the adoption of ad hoc concepts and solutions for the delivery of "cyber threat information/intelligence" (CTI), a product that provides its consumers with the (technical) understanding

Dr. Matteo E. Bonfanti is senior researcher at the ETH Center for Security Studies, Zurich.

of malicious networks operations and activities and enables them to take subsequent actions.[1] However, CTI alone does not prove to be fully suitable for supporting advanced prevention of cyberthreats.[2] 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 built and do not provide knowledge on the wider and articulated context within which cyber threats are framed.[3] They do not grant the understanding of cyber threat ecosystems nor do they enable advanced prediction/prevention.

By endorsing the idea that organizations should move from reactive to proactive security management postures and opposing the attitude to interpret cybersecurity mostly as "measures taken after-the-event" and "static perimeter defense," different representatives of the cybersecurity community are now sponsoring the adoption of concepts, tools, and practices for the crafting and sharing of all-encompassing intelligence about cyber threats.[4] 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 in the short, mid, and long terms, and take informed decisions on preventive actions to be taken. If integrated in their security-related decision-making processes, it should enable organizations to assume

1 Sharing of threat information, current attack patterns, software vulnerabilities and so forth have been standardized in process through the establishment of a network of CSIRTs (Computer Security Incident Response Teams). They have been augmented by the establishment and development of a number of initiatives, such as STIX/TAXII, CyBox, MISPs (Malware Information Sharing Platform). See, for example, http://stixproject.github.io/supporters/.

2 Brian P. Kime, "Threat Intelligence: Planning and Direction," *SANS Institute InfoSec Reading Room* (2017), p. 3, https://www.sans.org/reading-room/whitepapers/threatintelligence/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 defense.

3 See Michael Montecillo, "Why Context is King," *Security Intelligence*, April 22, 2014, https://securityintelligence.com/enterprise-it-security-context-king/.

4 The term "proactive" should be here understood as the capacity to address actual potential cyber threats by strengthening defense and response measures.

"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 labeled "cyber intelligence" (cyber INT or CYBINT) to differentiate it from the technically interpreted and narrow scope "cyber threat information/intelligence." In general, cyber intelligence is used to convey the idea of widely scoped and better qualified knowledge of actual or potential events regarding cyberspace that may endanger an organization.[5]

Similar to many other cyber-related notions, there is neither a crystallized definition nor a real common understanding of cyber intelligence—as a product and/or process—among policy makers, practitioner organizations, scholars, and public opinion. If one looks at the relevant policies or mechanisms that have been recently implemented (especially across Europe) as well as other documentation issued by private or public organizations and the academia, cyber intelligence is not always comprehensively defined and definitions vary.[6] Despite the growing use of this or similar expressions by the media as well as scholars and practitioners (especially by cybersecurity vendors for marketing reasons), current thinking on the subject is limited and not well developed. 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.[7] A deeper investigation of the subject—both from a theoretical and practical standpoint—is missing. On the contrary, the academic and practitioners' reflections on cyber intelligence are relatively more advanced among the

5 See also below.

6 Matteo E. Bonfanti, "Another –INT on the Horizon? Cyber intelligence is the New Black," paper presented at the Intelligence in the Knowledge Society Conference, Bucharest, October 26–27, 2017. An anthology of presented papers will be published in 2018.

7 At least this seems to be the case in some of the literature reviewed for the purpose of writing this paper. See, for example, Mario Caligiuri, *Cyber Intelligence. Tra libertà e sicurezza* (Roma: Donzelli, 2016); Mario Caliguiri, "Cyber Intelligence, la Sfida dei Data Scientist," June 2016, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/cyber 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* 3 (2013): 95–121; Umberto Gori and Luigi S. Germani, *Information Warfare 2011. La sfida della Cyber Intelligence al sistema Italia* (Bologna: Franco Angeli 2012).

US security and cybersecurity stakeholders.[8] This could be the consequence of the earlier adoption of cyber intelligence-related concepts, practices, and technological solutions by US-based organizations.[9] However, given that the push toward the adoption of cyber intelligence programs seems to be on the rise also among non-US cybersecurity stakeholders, it is worth expanding the discussion on this topic. In particular, it may be valuable to examine the notion of cyber intelligence in more detail as well as understand the implications arising from the employment of cyber INT-led approaches, methodologies, tools, and cooperation frameworks by national agencies and organizations.

The present paper intends to provide 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 existing analytical works on the topic. The paper reviews the available scientific literature addressing cyber intelligence, discusses the notion of cyber intelligence, and examines how it is crafted through the lens of the (cyber) "intelligence cycle." The paper concludes by stressing the need for a clear and shared understanding of cyber intelligence among relevant security and, especially, cybersecurity stakeholders.[10]

---

8 In addition to the literature that is cited below, see also discussion held by US cybersecurity stakeholders on the Cyber Intelligence Blog at https://cyberintelblog.wordpress.com/.

9 See, for example, Office of the Director of National Intelligence, "The National Intelligence Strategy of the United States of America," 2014, https://www.dni.gov/files/documents/2014_NIS_Publication.pdf. The strategy defines cyber intelligence as follows: "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." Ibid., p. 8. See also US Department of Defense Science Board, "Resilient military systems and the advanced cyber threat," January 2013, pp. 46 and 49, http://www.dtic.mil/docs/citations/ADA569975; US Department of Defense Science Board, "The Department of Defense Cyber Strategy," April, 2015, p. 24, https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

10 The paper is based on preliminary research that is currently carried out as part of a three-year research project defined and run by the author.

On Terminology and (Shared) Notions

In everyday language, "cyber intelligence" is mainly used as an enveloping and catch-all expression. What is cyber intelligence more exactly? As a product and a process, is it intelligence "from," "on," "within" or "for" cyberspace or some combination thereof? To what extent does it focus on this space or cover events/phenomena 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 issues associated with the crafting and sharing of 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. In general, reflections on cyber intelligence employ concepts, frameworks, and terminology derived from the intelligence community and adopt/adapt them to cyberspace.[11] This seems to be a logical approach given that some concepts are already established and there is no need to "re-invent the wheel." One may wonder, however, to what extent these concepts are applicable to a domain that differs from the traditionally known domains. Cyber is, in fact, a man-made, highly evolving, technologically shaped, and not fully tangible environment, which, perhaps, needs to be interpreted through different paradigms. Its interactions with the physical/real domain 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 experience on how it works and on the best capabilities to carry it out effectively. This hampers any attempt to come up with a thorough interpretative model for cyber INT.

The above considerations are important. They should not be disregarded by anyone who tried to adopt a less biased or uncertain approach to the study

11 Robert M. Lee, "An Introduction to Cyber Intelligence," (blog) *Tripwire*, January 16, 2014, https://www.tripwire.com/state-of-security/security-data-protection/introduction-cyber cyber intelligence/; Stephanie Helm, "Intelligence, Cyberspace and National Security," paper given at EMC Chair Symposium.

of cyber intelligence. They help in explaining why there is not yet an agreed and crystallized definition of cyber intelligence.

Cyber Intelligence: Actionable Knowledge "From" or "For" Cyber?

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 of looking at or interpreting cyber intelligence.[12] One way is to think about cyber INT as intelligence "from" cyber; that is, knowledge produced through the analysis of any valuable information collected "within" or "through" cyberspace. This is the 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 (for example, via Computer Network Exploitation technologies and techniques).[13] 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, and academia, including policy making, strategic planning, international negotiations, risk management, and strategic communication in areas beyond cybersecurity.[14] In other words, cyber intelligence may operate "independently and does not necessarily need to support a cybersecurity mission."[15] However, given that cyber intelligence is often discussed in relation to cybersecurity or the prevention of and response to cyber threats, these are the primary—but, again, not exclusive—goals of this type of intelligence.

12 Matthew M. Hurley, "For and From Cyberspace Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance," *Air & Space Power Journal* 26, no. 6 (2012): 12–33.

13 Ross W. Bellaby, "Justifying Cyber-Intelligence?" *Journal of Military Ethics* 15, no. 4 (2016): 299–319; Hurley, "For and From Cyberspace," p. 13. Computer Network Exploitation or cyber exploitation refers to the secret collection and reproduction of digital data from computers or networks.

14 Troy Townsend, Melissa K. Ludwick, Jay McAllister, Andrew O. Mellinger, and Kate A. Sereno, "SEI Innovation Center Report: Cyber Intelligence Tradecraft Project: Summary of Key Findings," (January 2013), pp. 2.01–2.20, spec. 2.5, https://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_40212.pdf.

15 Ibid.

Another way to interpret cyber INT is considering it as intelligence "for" cyber; that is, insight that is derived from an all-source intelligence activity occurring within and outside cyberspace. It is cyber intelligence lato sensu. In this sense, the intelligence "for" cyber can also include (or be built on) intelligence "from" 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 Intelligence (SOCMINT), and Human Intelligence (HUMINT).[16] 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 intended to inform decision makers on issues pertaining to activities in the cyber domain.[17] What qualifies this kind of intelligence as "cyber " is the purpose for which it is crafted: to support decision making on cyberspace-related issues.

The two discussed perspectives on cyber intelligence—intelligence "from" and "for" cyber—are often condensed into one single comprehensive concept. This is also due to the fact that intelligence "for" cyber actually incorporates the one "from" 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," "through," and/or "outside" cyberspace to enhance decision making on cyber-related menaces.

It is worth noting, however, that when looking at the "traditional" intelligence disciplines encompassed by the notion of cyber intelligence

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

17 Intelligence and National Security Alliance, "Operational Levels of Cyber Intelligence," September 2013, pp. 1–14, https://www.insaonline.org/operational-levels-of-cyber cyber intelligence/. See also Intelligence and National Security Alliance, "Cyber Intelligence: Setting the Landscape for an Emerging Discipline," September 2011, pp. 1–20, https://www.insaonline.org/cyber cyber intelligence-setting-the-landscape-for-an-emerging-discipline/. On the existing intelligence disciplines, see, among others, the UK Ministry of Defence, "Understanding and Intelligence Support to Joint Operations," Joint Doctrine Publication 2-00, August 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

lato sensu, their narrower and circumscribed projection on cyberspace has determined the development of ad hoc concepts and approaches often referred as virtual HUMINT, virtual or internet-based OSINT, virtual COMINT, and so forth. The adjective "virtual" indicates that intelligence activities are carried out within the cyberspace or through computer-generated tools. The association of "virtual" with "traditional" INT concepts/practices refers to the adoption of methods/approaches/tools that are employed by these latter practices and adapted for cyberspace.[18] A bit different from the above concepts is the notion of SOCMINT. According to some scholars/practitioners, SOCMINT is as a stand-alone discipline that has specific features.[19]

As for the information for crafting cyber intelligence, this may range from network technical data (for example, hardware and software data), data on hostile organizations and their capabilities, ongoing cyber activities, to potentially any relevant data on geopolitical events.[20] The type of data as well as its classification are not functional to the definition of cyber intelligence. Data can be raw or already processed information; it can be obtained legally or through unlawful intrusion/exploitation actions from open, proprietary, or other classified sources.[21] As the literature suggests, multiple sources of information are needed to develop a more holistic understanding of the threat environment and to produce a comprehensive cyber INT.[22] The most important aspect of the data is that it should be somehow validated. When analyzed, information should allow decision makers to identify, track, and predict cyber capabilities, intentions, and activities that offer courses of

18 For example, the virtual HUMINT approach aims at collecting tactical/operational intelligence from the information generated by members of virtual communities.

19 David Omand, Jamie Bartlett, and Carl Miller, *#Intelligence* (London: Demos Publishing, 2012). See also, Matteo E. Bonfanti, "Social Media Intelligence a Salvaguardia dell'Interesse Nazionale. Limiti e Opportunità di una Pratica da Sviluppare," in *Intelligence e Interesse Nazionale*, ed. Umberto Gori and Luigi Martino (Rome: Aracne, 2015), pp. 231–262.

20 Jung-ho Eom, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace," *International Journal of Software Engineering and Its Applications* 8, no. 9 (2014): 137–146. This article deals with cyber intelligence for military purposes.

21 Robert M. Lee, "Cyber Intelligence Collection Operations," 2014, https://www.tripwire.com/state-of-security/security-data-protection/cyber cyber intelligence-collection-operations/.

22 Intelligence and National Security Alliance, "Cyber Intelligence," p. 1.

action.[23] This is the main feature of cyber intelligence; that is, the enabling goal of providing its consumers with insight into potentially hostile activities that may occur in the cyber domain or may be perpetrated through or against cyberspace, allowing them to design effective preventive (proactive) or counteractive (reactive) measures.

Depending on its scope or level of actionability, cyber intelligence can be strategic, tactical, or operational.[24] There is no uniform interpretation of what the different levels of cyber INT should consist. According to the available literature, strategic cyber INT focuses on the long term. Typically, it reviews trends in current and emerging threats and examines opportunities to contain these threats. It serves apical decision-making processes aimed at achieving an organization's mission and determining its direction and objectives. Strategic cyber INT covers the threat landscape for macro trends (political, social, and economic) affecting the organization and identifies the threat actors, their goals, and how they may attempt to achieve them; it is rich in contextual information.[25] Tactical cyber intelligence concerns what happens on the network. It also examines the strength and vulnerabilities of an organization, and the tactics, techniques, and procedures (TTPs) employed by the threat actors.[26] Due to its nature and reach, tactical cyber INT corresponds generally to cyber threat intelligence.[27] Generally more technical in nature, it informs the specific network-centered steps and actions the organization can take to protect assets, maintain continuity, and restore operations. As far as operational cyber INT is concerned, it consists of knowledge of imminent or direct threats to an organization. It enables and

23 Townsend et al., "SEI Innovation Center Report."

24 See for example, Randy Borum, "Getting 'Left of the Hack': Honing Your Cyber Intelligence Can Thwart Intruders," InfoSecurity Professional (September/October 2014), https://works.bepress.com/randy_borum/63/.

25 Randy Borum, John Felker, Sean Kern, Kristen Dennesen, and Tonya Feyes, "Strategic Cyber Intelligence," *Information & Computer Security* 23, no. 3 (2015): 317–332. See also, Intelligence and National Security Alliance, "Strategic Cyber Intelligence," March, 2014, pp. 1–16, https://www.insaonline.org/strategic-cyber cyber intelligence/.

26 Intelligence and National Security Alliance, "Tactical Cyber Intelligence," December, 2015, pp. 1–16, https://www.insaonline.org/tactical-cyber cyber intelligence/.

27 Ibid.

sustains day-to-day operations and output. At this level, cyber intelligence looks at the organization's internal processes and vulnerabilities.[28]

It is 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.[29] Regardless of any clear-cut demarcation between the levels, the capacity of an organization 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 is quite important. As a finished product, it seems there are no established formats or standards for presenting cyber intelligence to decision makers.

The Cyber Intelligence Process: Alternative vs. Traditional Models

Just like in the case of other intelligence products/disciplines, cyber intelligence is crafted through a set of activities/functions. Traditionally, this set of activities/functions is represented and explained through the "intelligence cycle" model.[30] The model has been studied and questioned several times by practitioners and academics to the point that alternative models have

28 Intelligence and National Strategic Alliance "Operational Cyber Intelligence," October, 2015, pp. 1–16, https://www.insaonline.org/operational-cyber cyber intelligence/.

29 Intelligence and National Strategic Alliance, "Strategic Cyber Intelligence," p. 4.

30 While there are different representations of the intelligence cycle, the most common comprises five distinct functions: Planning and Direction, Collection, Processing, Analysis, and Dissemination. Some of these functions may be further broken down, thus making the overall cycle consisting of Planning and Direction, Collection, Collation, Evaluation, Analysis, Integration, Interpretation, and Dissemination. On the intelligence cycle, see Mark Phythian, ed. *Understanding the Intelligence Cycle* (London and New York: Routledge, 2013). In particular, see Philip H.J. Davies, Kristian Gustafson, and Ian Ridgen, "The Intelligence Cycle is Dead, Long Live the Intelligence Cycle," in *Understanding the Intelligence Cycle*, p. 56.

been proposed and discussed.[31] The "validity/applicability" of the traditional intelligence cycle is also questioned in the context of cyber intelligence. As one eminent expert noted, "as intelligence grows ever more digitalised and 'cyberised' (in its subject matter, its methods, and its forms), a clearer understanding that the Intelligence Cycle is actually quite a dated heuristic device—rather than a constructive dimension of intelligence as such—can liberate *stakeholders* to think about intelligence in more innovative ways."[32] This view is shared by other scholars and experts. They stress the limited applicability of the model to intelligence generated "from" and "for" cyber; they underline its inability to represent and explain the crafting process of cyber intelligence. Meant as a linear and reiterative cycle, the traditional model does not emphasize the inter-related nature of the activities (planning, collection, processing, and so forth) that the cyber intelligence process consists of and their mutual relevance; in other words, it does not capture their inter-dependencies and mutual influences.

Actually, the above critics draw from arguments that are made for describing the inadequate representativeness of the intelligence cycle in general, regardless of the specific INT discipline at stake.[33] Therefore, one may question more in-depth if and why an ad hoc interpretative model is necessary to explain the cyber intelligence process; or, in other words, if and why the cyber INT process is so peculiar and different from the processes embedded in other INT disciplines that it requires being described through an alternative model. Providing consistent answers to the above questions would require a clear, comprehensive, and thorough understanding of cyber INT as a concept and, above all, as a practice. Such an understanding is difficult to reach due to the lack of enough reflections and experience in cyber INT. Therefore, at the current stage, the definition of an interpretative model

31 On the flaws of the traditional intelligence cycle in representing any intelligence process, see the different contributions in Phythian, ed. *Understanding the Intelligence Cycle*. It is worth noting that all models lack accuracy because they are simplifications of complex realities. Furthermore, models are not processes; rather, they are reduced representations of processes. Therefore, it does not makes sense to expect from the intelligence cycle model—as well as any other potential model—to provide an holistic, all-encompassing, and fully detailed representation of the intelligence process. Such models would be incredibly complex and have low practical value.

32 Michael Warner, "The Past and Future of the Intelligence Cycle," in *Understanding the Intelligence Cycle*, p. 19.

33 Phythian, ed. *Understanding the Intelligence Cycle*.

represents mostly a sort of intellectual exercise or a test whose results should be progressively validated. Nonetheless, some arguments seem to support well the definition of an ad hoc model to explain the cyber INT process.

Tautologically speaking, the main feature of cyber INT lies in the fact that it is "cyber centered"; that is, it is knowledge concerning cyber-related issues. Cyber INT involves the analysis of information collected from cyberspace as well as from other sources for achieving cyber-related purposes. At the very basic level, the adjective "cyber" refers to a man-made, highly evolving, technologically shaped and not fully tangible domain.[34] In this domain, information is generated, processed, disseminated, shared, stored, altered, consumed, and destroyed by a multitude of actors at an incredible speed.[35] The impact of targeted decision making on cyber-related issues and its effects on both the virtual and physical domains are difficult to foresee. This affects the way in which cyber intelligence is crafted and consumed. It challenges the core functions of the intelligence process when applied to the cybersphere, namely, the collection, evaluation, analysis, integration, interpretation of information, and dissemination of intelligence.

With regard to the collection and evaluation, cyber intelligence relies also on information delivered by uncontrolled sources, such as the internet.[36] This information should be filtered, evaluated, and (somehow) validated. Filtering is paramount in order to select only significant items of information from cyberspace. Evaluation is often a challenging task due to the high volatility, anonymity, and uncertainty of data available in cyberspace and

34 This domain is both an element and the result of the digital revolution. See Luciano Floridi, *Information: A Very Short Introduction* (Oxford: Oxford University Press; 2010); Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford: Oxford University Press, 2016).

35 Warner, "Past and Future of the Intelligence Cycle," p. 16.

36 Collection can be defined as the exploitation of sources and the delivery of the information obtained for processing and analysis. A source can be a person, object, process, or system from which information can be obtained. Sources are uncontrolled when they are not under formal supervision and direction of an organization. One may think of information generated by internet users or other actors in cyberspace. Evaluation can be defined as a phase in the analysis function that constitute the appraisal of an information in respect of the reliability of the source and the credibility of the information. See, for example, the UK Ministry of Defence, "Understanding and Intelligence Support to Joint Operations," Joint Doctrine Publication 2-00, August, 2011, pp. 3-14 and 3-20, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/311572/20110830_jdp2_00_ed3_with_change1.pdf.

the heterogeneity of data sources. To validate data, it becomes therefore paramount to corroborate the information derived from one source with that derived from other sources, and it is better if at least one of the former is controlled. Filtering, evaluation, and validation aim at mitigating the so-called "information anarchy" generated by the increasing volume of available data coupled with the lack of control over them. Given that the crafting process of cyber intelligence may also draw on information/intelligence produced through other disciplines, the integration of all relevant pieces of knowledge into one single and consistent product can be challenging. This is due to the different format, nature, and grade of uncertainty of information and intelligence obtained from cyberspace (for example, information or other technical data sourced from social media, web forums, and so forth) confronted with other "non-virtual" sources.[37] The grade of uncertainty affects also the interpretation of processed information; that is, the judgment and deductions based on it, which are generally added in the final cyber INT product. Such uncertainty should also be clearly conveyed to the consumer of cyber intelligence, who should be aware of its main limits in terms of accuracy.

Another relevant aspect to be considered when defining any interpretative model for the cyber INT process is the tight time frame that often is required for executing intelligence functions. This demands that functions occur simultaneously or that shortcuts are taken in their execution. In other words, functions do not run in a circle but establish an "all-channel network" among themselves.[38]

The above-discussed requirements of the cyber INT crafting process—and the challenges they pose—seem to prompt the definition of a specific interpretative model that could better capture the peculiarities of the process. By looking at the literature, a team of experts and academics working at the Software and Engineering Institute (SEI) of the Carnegie Mellon University proposed their own model a couple of years ago.[39] The SEI model differs from the traditional intelligence cycle because of the adopted terminology, the non-linear and strictly consequential logic of the functions the process

37 Integration can be defined as the function on the intelligence process whereby analyzed information and /or intelligence is selected and combined into a pattern in the course of the production of further intelligence. Ibid. p. 3–22

38 See, for example, Philip H.J. Davies, Kristian Gustafson, and Ian Ridgen, "The Intelligence Cycle is Dead, Long Live the Intelligence Cycle," p. 64 ff.

39 Townsend et al., "SEI Innovation Center Report."

consists of, the breakdown of the analysis function into two specialized functions (the technical or functional analysis and the strategic analysis), and the capacity to capture both the "narrow" technical cybersecurity and the "wider" cyber threats-prevention purposes that cyber intelligence can serve within an organization. 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 that is intended to inform decision makers on issues pertaining to activities in the cyber domain.[40] The SEI model consists of five functions: (1) the determination of the "environment" that establishes the scope of the cyber intelligence effort and influences what information is needed to accomplish it;[41] (2) the "data gathering" or the exploration of data sources and collection and filtering of information through automated and labor-intensive tools;[42] (3) the "functional analysis," which is the performance of technical and tailored analysis (typically in support of a cybersecurity mission) aimed at deriving the "what" and "how" of cyber threats;[43] (4) the "strategic analysis" entailing the review, integration with contextual information, and further elaboration of the functional cyber intelligence with the goal of answering

40 Ibid.

41 Ibid., p. 2.9. Environment is meant as both internal and external. The determination of the internal environment includes the studying of an organization's global cyber presence, the infrastructure that is 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 entities are capable of affecting organizations' networks. It must find out and map system vulnerabilities, intrusion or network attack vectors, the tactics, techniques, procedures, and tools used by relevant threat actors. As it is suggested in Townsend et al., "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."

42 Ibid., p. 2.11. Data gathering should cover both internal (net-flow, logs, user demographics) and external sources (third-party intelligence providers, open source news, social media). It should focus on the pertinent threats and strategic needs identified while learning about their organization's environment. Indeed, 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.

43 Ibid., p. 2.13. This function includes the verification/validation of data based on the quality of the source, reporting history, and independent verification of corroborating sources.

the "who" and "why" questions;[44] and (5) the "reporting and feedback"; that is, the dissemination of cyber intelligence to decision makers and the collection of feedback.[45]

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 organization on the basis of cyber intelligence consumed. The intelligence resulting from the functional analysis can inform decisions on actions to be taken at the technical-network level of an organization which, in turn, impact on the determination of the internal environment; the same goes for intelligence resulting from the strategic function, which affects 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 that contributes in bridging the communication gap between analysts and top decision makers. The latter provide feedback on the intelligence received in order to shape analytical functions, adjust the direction of the organization, and therefore influence the environment.

Questioning the "validity" of the SEI model is beyond the scope of this paper. The model was designed and proposed as a result of empirical work that mapped and assessed current practices in US cyber intelligence. It is grounded in data and represents the state of the art within selected US-based organizations. It has also a normative reach; that is, it suggests how the process should work to be effective. Furthermore, the proposed model has the advantage of being relatively simple while, at the same time, representative of practices adopted by different types of organizations, such as small corporations, larger industries, and governmental agencies. However, its representativeness is likely to fade away at both the lower and higher levels—the individual and multi-partnership or transnational levels—of

44 Ibid., 2.15. Strategic analysis adds perspective, context, and depth to functional analysis. It is ultimately rooted in technical data but incorporates 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.

45 Ibid., p. 2.17.

occurrence of the cyber intelligence process. Especially at the latter level, the degree of organizational/institutional complexity will probably render the intelligence model unfit. In addition, technological developments in the field of cyber will probably affect the model and require further (periodical) re-elaborations.[46] Lastly, the proposed model still suggests that collection and analysis are sequential; that is, the latter can only begin once the former is complete. In practice, the two functions are interactive and occur concurrently. That being said, one may acknowledge that the SEI proposed model represents a sound and initial attempt to better explain how cyber intelligence is and should be crafted.[47]

Conclusion

Having a clear understanding of cyber INT is important. It can help relevant stakeholders to be consistent when they promote programs or take actions concerning cyber intelligence at the policy, legal, operational, and other levels. Such understanding should be premised upon the definition of a sound conceptual framework of cyber intelligence. This framework should serve as a structure to be employed for making conceptual distinctions, organizing ideas, and interlinking them to provide a comprehensive understanding of cyber intelligence. The adoption of such a framework would also represent a paramount element to develop cyber INT as a discipline; that is, a specific area of study or work in intelligence. Although most of the literature considers cyber INT as being an already-established or soon-to-be-established discipline, it does not seem to be the case. The lack of a more mature theoretical elaboration of cyber INT, coupled with the relatively limited experience in it, makes it difficult to consider this type of intelligence as a recognized area or branch of intelligence. In other words, cyber INT should not be considered a discipline because it has not yet been sufficiently theoretically defined nor 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

46 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."

47 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.

course, nothing prevents cyber INT from establishing itself as a discipline that employs specific technical or human resources throughout the different functions of its crafting process.

Finally, a shared understanding of cyber INT becomes a prerequisite when relevant stakeholders aim at establishing cooperation mechanisms in the field. This latter aspect is quite important. Indeed, the crafting process of cyber intelligence ideally requires mutual collaboration and knowledge sharing. 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.

By defining cyber intelligence stricto or lato sensu (according to the already produced knowledge on the topic), identifying and structuring its conceptual components, as well as representing/interpreting them through a very basic (and preliminary) theoretical framework, the present paper contributes to explaining cyber INT. Needless to say that a more profound articulation of the framework is needed in order to grasp the different facets of cyber intelligence and better understand how this emerging practice could be established and further evolve.