BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Development of a Cyber Threat Intelligence apparatus in a central bank

by Pasquale Digregorio and Boris Giannetto

October 2019

Number 517

BANCA D'ITALIA
EUROSISTEMA

Questioni di Economia e Finanza

(Occasional Papers)

Development of a Cyber Threat Intelligence apparatus in a central bank

by Pasquale Digregorio and Boris Giannetto

Number 517 – October 2019

The series Occasional Papers *presents studies and documents on issues pertaining to the institutional tasks of the Bank of Italy and the Eurosystem. The* Occasional Papers *appear alongside the* Working Papers *series which are specifically aimed at providing original contributions to economic research.*

The Occasional Papers *include studies conducted within the Bank of Italy, sometimes in cooperation with the Eurosystem or other institutions. The views expressed in the studies are those of the authors and do not involve the responsibility of the institutions to which they belong.*

The series is available online at www.bancaditalia.it .

ISSN 1972-6627 (print)
ISSN 1972-6643 (online)

Printed by the Printing and Publishing Division of the Bank of Italy

DEVELOPMENT OF A CYBER THREAT INTELLIGENCE APPARATUS IN A CENTRAL BANK

by Pasquale Digregorio and Boris Giannetto*

Abstract

The present work defines the development of a cyber threat intelligence (CTI) apparatus in a central bank. Such a system aims at promoting a preventive posture against constantly evolving threats such as cybercrime, cyber espionage, hacktivism, cyberterrorism and state-sponsored APTs. Central banks are targeted by a gamut of threat actors. Cyber-attacks against financial institutions are on the rise: Those directed against strategic data, infrastructures and platforms of a central bank, could have momentous repercussions on the vital ganglia of the financial system as a whole. CTI operates on a three-level scale: Tactical/technical, operational and strategic. As to the latter, geopolitical and context analysis is key. The proposed CTI apparatus - designed to cope with multifarious cyber threats - aims at spurring systemic prevention and resilient reaction

JEL Classification: F50, G38, K24, L50, O33.
Keywords: cyber threat intelligence, cyber intelligence, geopolitical analysis, complex adaptive systems, cybersecurity, cyber resilience.

Contents

* Bank of Italy, Directorate General for Information Technology, IT Planning Directorate, CERT

1. Introduction[1]

In recent years, cyber threats have been considerably evolving. This phenomenon is linked to the increasing exploitation of opportunities offered by cyberspace (e.g. reduction of space-time limits and lower costs) for the achievement of political, military and economic goals by diversified actors (states, intelligence agencies, private companies, organized crime and netizens).

Escalation of asymmetric and hybrid warfare, including potential cyber-attacks against critical financial infrastructures, is a growing national security concern in many countries.

On a global level, cyber-attacks directed towards financial institutions are on the rise and a continuous evolution in the sophistication of attack vectors is in progress. These phenomena are catalyzed by growing capabilities of well-endowed and high motivated threat actors, software re-use of governmental tradecraft available in the wild and possibility to have recourse to cybercrime as-a-service.[2]

Structure, speed and meta-polymorphism of these attacks make a paradigm shift necessary: One ought to move from a classic approach focused on risk management, to a posture based on preventive threat management.

In this regard, a zero risk condition is not a viable path. Considering the current international scenario, characterized by a high degree of interconnection between diverse threats, an approach based on risk probability may prove inaccurate and ineffective.

On the contrary, the development of a cyber threat intelligence (CTI) apparatus, which is complementary to classic cybersecurity measures, could serve the purpose.

Cyber threat intelligence is a proactive activity, aimed at collecting and analyzing heterogeneous data, coming from different internal and external information sources: Its main objective is to extract useful information for decision makers. CTI helps an organization or institution to assign a specific threat profile to its assets and to develop effective counter-actions.

In particular, CTI activities are carried out by collecting, classifying, integrating and analyzing cyber threats raw data. This process is aimed at producing useful information for constituency (internal CTI user base), through investigations on threat actors, possible real motivations, connections between clusters of events, tactics, techniques and procedures (TTPs) used by the attackers.

[1] We would like to thank Ebe Bultrini, Luigi Cannari, Arturo Baldo, Riccardo Cristadoro and Sabina Di Giuliomaria for their insightful observations and editorial advice.

[2] The term “tradecraft” refers in general to techniques, methods and technologies used in espionage and intelligence activities; in the cyber domain, it could include, for example, a particular malware or a form of encryption. In cybersecurity, the locution “in the wild” indicates, by and large, publicly used tools. The phrase “cybercrime as-a-service” means that people/companies/governments could pay criminal providers to launch cyber-attacks.

2. Global trends and threats in the cyber domain

The cyber domain represents a transversal dimension, often strongly intertwined with other domains and threats of different nature.

Classic domains (land, sea, air, space) are all intimately tangled with the cyber component, which therefore goes to configure a sort of cross domain.

With regard to global threats, they are often simultaneous and complementary: As a result, hybrid phenomena arise and cyber threats are often means that sustain other (financial, economic, political, ideological, military, criminal) threats.

2.1 Current Trends

Cyberspace has significantly changed since the first cyberattack in the Internet age occurred (Morris Worm, in 1988). From area without boundaries (both at technical and regulatory level), it has gradually become a *de facto* subdivided space, with ever more clear and (sometimes opposed) sovereignties.

On the one hand, the idea of *superiorem non recognoscens* state based on sovereignty, people and territory, has been put to the test by borderless cyberspace, cryptocurrencies and netizenship; on the other hand, the so-called “national Internet” is becoming an increasingly debated and popular topic, with concrete implications in some states.

This stance is complemented by confrontational cyber strategies and tactics. Some national cyber strategies even imply the possibility for governmental entities, under certain circumstances, to field active defense measures or to obtain information from national private companies, on a mandatory base.

As to tactics, geoblocking of IP addresses against significant “attack traffic”, originating from geopolitical rivals or from the dark web, is implemented in some major countries.[3]

The transnational nature of the network (web, deep web, dark web) poses significant problems. The global Internet governance appears to be a conundrum, that can only be solved through international concerted actions and innovative regulatory instruments, except for national interests.

[3] Geoblocking indicates a measure aimed at blocking Internet traffic or limiting Internet access, on the basis of geographical location. A more targeted way of blocking, that allows to ban a part of the entire traffic of a country, is focused only on malicious Autonomous System Numbers (ASN). With regard to the dark web, an example of restriction consists in blocking Tor exit nodes. Tor (acronym of "The Onion Router") is a free and open-source software, that enables anonymous communication and traffic: It is a darknet, part of the dark anonymous web.

Gaps in public and private international law, mismatch between law enforcement in physical and virtual space, unregulated or loose-regulated social networks platforms are just few examples of legal hitches.

Technical standards, economic polarization, net neutrality, revenue sharing, (big) data management and privacy are other intrinsic difficulties of the global Internet.

In the last few years, public opinion has been becoming increasingly favorable to a state regulatory intervention in social networks privacy policies and in data privacy matters in general.[4]

Furthermore, a moot aspect - to be investigated even more carefully in the years and decades to come - is given by social and psychological impacts of the Internet on people's mindset and on collective behaviour.[5]

The psychosocial factor may prove to be an even greater puzzle and security issue than "echo chambers", "trolls" and deliberate interstate interference campaigns.[6]

Nowadays, the cyber domain complements classical domains of warfare. A progressive equivalence between territorial space and cyberspace creates a parallelism between territorial sovereignty and cyber sovereignty, even if internationalism endures and permeates discussions about the global network governance.

At inter-state level, cyberwarfare is in the meantime evident and underground: It takes on the contours of dissimulated drills, but it is also part of real hybrid war, where objectives and disruptive means of attack become multiple.

In this milieu, boundaries between states and cybergangs get mixed up, with employment of similar TTPs. Wannacry and Petya Not Petya could be glaring examples.[7]

Typical cyberwarfare actions include, for instance, massive cyber-attacks against critical infrastructures, economic cyber espionage, cyber sabotage, exfiltration and manipulation of data, disinformation campaigns, political pressure through information operations, cyber counterintelligence.[8]

[4] The Cambridge Analytica case and the Marriott/Starwood data breach strengthened this sentiment.

[5] As to emergent behaviour, the term "sheeple" (crasis from sheep and people) well indicates the docile, easily influenced and led mass of global Internet users. Means have become ends and the Internet medium has become an objective. With regard to state interference campaigns, examples are offered by computer network operations (CNO) and psychological operations (PSYOP).

[6] The phrase "echo chamber" depicts a situation in which beliefs are amplified or reinforced by communication and biases inside a closed system (e.g. a social network community). The term "troll" indicates, on the whole, a person who sows discord in an online community, with deliberately provocative and inflammatory messages.

[7] The WannaCry worldwide ransomware cyber-attack was launched in May 2017. Not Petya was a major global cyberattack occurred in June 2017, utilizing a new variant of the Petya ransomware.

[8] Cyberwarfare is a set of actions - carried out by state actors, sometimes in conjunction with non-state actors, such as cybergangs or cyberterrorists - aimed at acquiring superiority in the cyber domain or at damaging adversaries. It could be part of a wider warfare strategy, based on multiple purposes and diverse means of attack (hybrid cyberwarfare).

In this scenario, in order to curb foreign possible interference, some countries have raised controls on foreign devices and equipment, for avoiding espionage or supply chain attacks.[9]

Nation-state and state-sponsored cyber-attacks are on the rise. Without getting through sensational episodes (just a mention to the striking cyber heist of the central bank of Bangladesh), a growing confrontation is underway, with international actors being at the same time offender and victim. Cyber postures appear increasingly aggressive, with episodic judicial indictments.

Structured attacks stem from diversified phenomena such as cybercrime, cyberterrorism, hacktivism, interstate cyberwarfare and state-sponsored APT (Advanced Persistent Threats).

In this context, relying on the only technical analysis of a cyber-attack turns out to be ineffective, because of limited and volatile digital evidence, peculiarities of cyberspace, anonymization, obfuscation and antiforensics techniques developed by threat actors.[10]

Geopolitical and context analysis can help digital investigations both *ex ante* and *ex post*. It can spur technical analysis with situational cues; it can also provide information about campaigns before technical indicators identify cyber events or even before cyber-attacks occur (top-down approach). In addition, it can contextualize attacks, by analyzing trends, real motivations and links between cyber events, while examining attributions to threat actors; it can thwart possible geopolitical interference in threat intelligence data feeds (bottom-up approach).

There could be, at any rate, “false flags” operations, carried out with the intention of making believe that an attack is attributable to another actor (by employing TTPs usually used by that actor).[11]

The aforementioned attribution difficulties often translate into a “plausible deniability” condition. These ambiguities make the use of cyberspace particularly profitable even for warfare covert activities.

As far as attributions are concerned, international CTI analysts usually have recourse to conventional names (e.g. APTs)[12], that are linked - presumptively or on the basis of conclusive evidence - with real actors.

[9] A supply chain cyber-attack targets elements in the supply network, through the installation of a rootkit or hardware-based spying components. These kind of attacks usually are divided in seeding attacks (production phase of the supply chain) and interdiction attacks (logistics phase of the supply chain).

[10] Examples of anonymization techniques are encrypted channels, proxy and virtual private networks (VPN). These techniques could make vain any forensics effort: For instance, it could be difficult or not possible to trace real IP chains.

[11] Furthermore, a malware code could be re-used by another actor, without the intent of deceiving and disguising about the blame for attacks. False flags and antiforensics obviously do not exclude the use of "own" (real and non-disguised) infrastructures and IPs: These can be especially employed in transnational actions, due to the difficulty to attribute and legally prosecute in different jurisdictions.

[12] For instance, APT1 and APT10, APT28 and APT29, APT33 and APT34, APT37 and APT38.

Below (Figure 1) we propose a representation, on a global scale, of the current main APT clusters divided by country: The attributions are those considered most plausible.

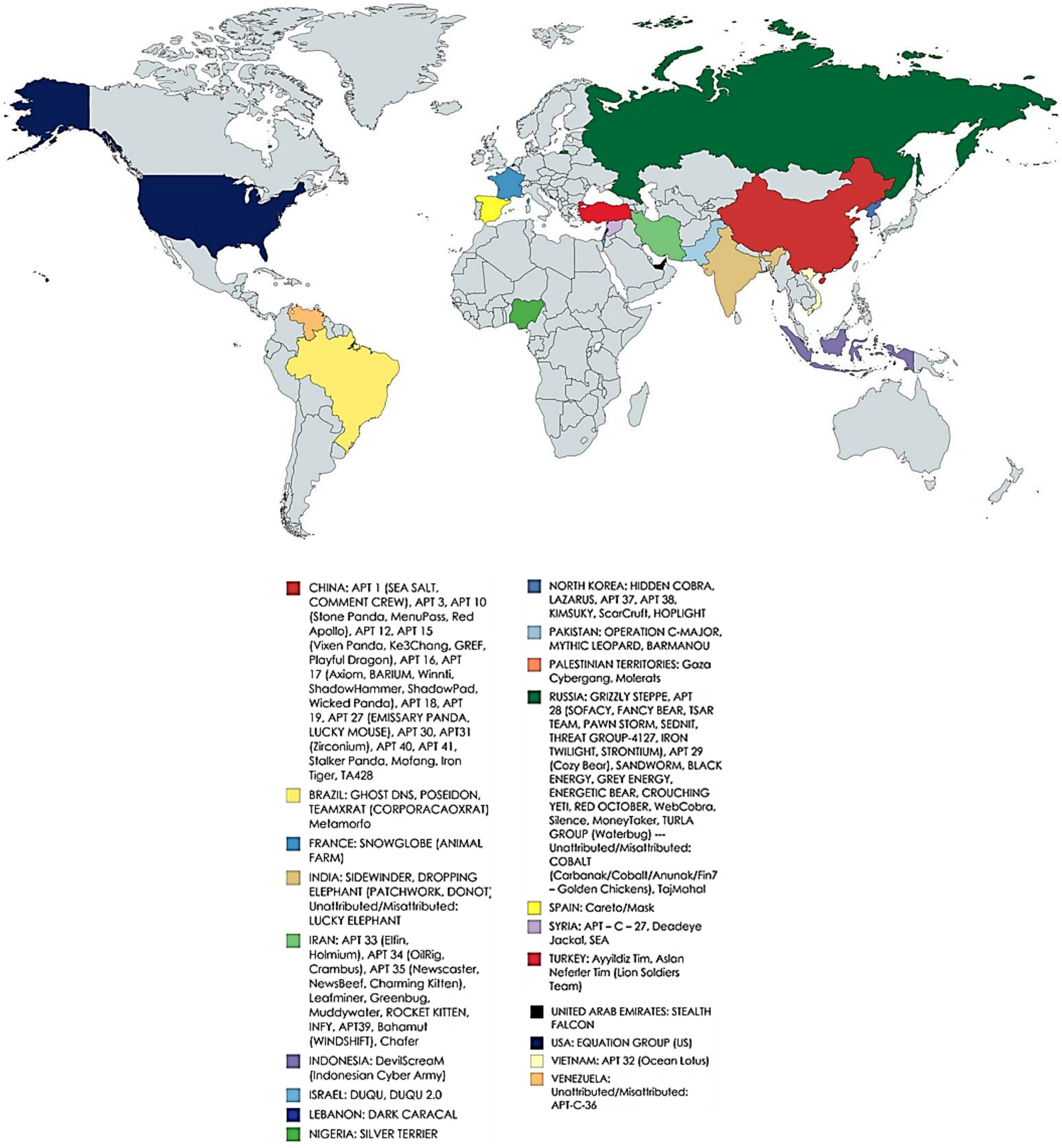

🟥 CHINA: APT 1 (SEA SALT, COMMENT CREW), APT 3, APT 10 (Stone Panda, MenuPass, Red Apollo), APT 12, APT 15 (Vixen Panda, Ke3Chang, GREF, Playful Dragon), APT 16, APT 17 (Axiom, BARIUM, Winnti, ShadowHammer, ShadowPad, Wicked Panda), APT 18, APT 19, APT 27 (EMISSARY PANDA, LUCKY MOUSE), APT 30, APT31 (Zirconium), APT 40, APT 41, Stalker Panda, Mofang, Iron Tiger, TA428
🟨 BRAZIL: GHOST DNS, POSEIDON, TEAMXRAT (CORPORACAOXRAT) Metamorfo
🟦 FRANCE: SNOWGLOBE (ANIMAL FARM)
🟫 INDIA: SIDEWINDER, DROPPING ELEPHANT (PATCHWORK, DONOT; Unattributed/Misattributed: LUCKY ELEPHANT
🟩 IRAN: APT 33 (Elfin, Holmium), APT 34 (OilRig, Crambus), APT 35 (Newscaster, NewsBeef, Charming Kitten), Leafminer, Greenbug, Muddywater, ROCKET KITTEN, INFY, APT39, Bahamut (WINDSHIFT), Chafer
🟪 INDONESIA: DevilScreaM (Indonesian Cyber Army)
🟦 ISRAEL: DUQU, DUQU 2.0
🟦 LEBANON: DARK CARACAL
🟩 NIGERIA: SILVER TERRIER
🟦 NORTH KOREA: HIDDEN COBRA, LAZARUS, APT 37, APT 38, KIMSUKY, ScarCruft, HOPLIGHT
🟦 PAKISTAN: OPERATION C-MAJOR, MYTHIC LEOPARD, BARMANOU
🟧 PALESTINIAN TERRITORIES: Gaza Cybergang, Molerats
🟩 RUSSIA: GRIZZLY STEPPE, APT 28 (SOFACY, FANCY BEAR, TSAR TEAM, PAWN STORM, SEDNIT, THREAT GROUP-4127, IRON TWILIGHT, STRONTIUM), APT 29 (Cozy Bear), SANDWORM, BLACK ENERGY, GREY ENERGY, ENERGETIC BEAR, CROUCHING YETI, RED OCTOBER, WebCobra, Silence, MoneyTaker, TURLA GROUP (Waterbug) --- Unattributed/Misattributed: COBALT (Carbanak/Cobalt/Anunak/Fin7 – Golden Chickens), TajMahal
🟨 SPAIN: Careto/Mask
🟪 SYRIA: APT – C – 27, Deadeye Jackal, SEA
🟥 TURKEY: Ayyildiz Tim, Aslan Neferler Tim (Lion Soldiers Team)
⬛ UNITED ARAB EMIRATES: STEALTH FALCON
⬛ USA: EQUATION GROUP (US)
⬜ VIETNAM: APT 32 (Ocean Lotus)
🟧 VENEZUELA: Unattributed/Misattributed: APT-C-36

Figure 1 – Current main APT clusters by country: Attributions deemed most plausible

Conventional names are often multiple for the same threat actor: Each organization uses specific tags, on the basis of different naming criteria (as indicated in Figure 2, conventional APT names are also referred to by other names). This occurrence puts to the test the CTI analysts' attribution activity, especially in the absence of unambiguous evidence.[13]

The most effective tools - that allow to leave the field of plausibility - for achieving evidence ("smoking guns") about threat actors, are often only available to law enforcement and intelligence agencies.

However, collecting clues and carrying out CTI activities, helps to understand threat scenarios, with plausible attack matrices and sometimes conclusive results.[14]

Analyzing attributions and threat actors is a challenging test, sometimes without consequence: It is however a key element in CTI activities. It is important to understand who launched an attack, how the attack was launched and why; a defense against artifacts coming from unknown threats cannot last long.[15] Attribution and contextualization often support in identifying the best technical and tactical tools to prevent, detect and respond.

In any case, the above-mentioned false flags and disinformation techniques often transform the international cyber arena into a hall of mirrors, fueled by deterrence, public allegations, hybrid warfare and covert attacks.[16]

Cyber activities of actors such as Hidden Cobra, Grizzly Steppe and Stone Panda - as well as their alleged links with governmental bodies - are now in the public domain. In parallel, states make more and more public their cyber capabilities.

In this regard, the mounting tendency to publicly accuse other countries for cyber-attacks and the mentioned greater bent to go public denote the implementation of systematic deterrence strategies.

2.2 Cyber Threats to the Financial Sector

With specific regard to the financial sector, cyber-attacks show a growing trend. Financial institutions are targeted by a gamut of threat actors and face multifarious threats, because of their role in intermediating funds and regulating markets.

[13] In any case, one ought to bear in mind that at a certain level of investigation, it makes little sense to talk about APTs, since especially in the case of state actors, specific governmental entities are behind conventional names.

[14] CTI analysts who work in public administrations and private companies could therefore also act as "sensors": A sort of national prevention and defense front line, for possible subsequent verifications and actions by law enforcement and intelligence agencies.

[15] This approach would be equivalent to fighting an antigen, without knowing the viral strain from which it stems.

[16] In this scenario, analysis on attribution of cyber-attacks gives rise to - sometimes apparent, sometimes real - superposition of states (intended both as simultaneous conditions that exist at a particular time and as blocs of countries and governments that operate simultaneously). At any rate, the whole cyber landscape is destined to change with the widespread introduction of groundbreaking technologies, such as those based on quantum computing, that have the potential to dramatically alter cryptography and communication patterns. Post-quantum cryptography models are intended to address this topic.

This variegated set of threats requires a constant and full-fledged analysis effort, to continuously adapt the organizations' defense and prevention capabilities.

In this context, designing a threat model for a central bank is a highly challenging, time-spending and non-stop activity.

Threat modeling aims at defining potential threats, while highlighting vulnerabilities of an institution/organization, from attackers' point of view. In addition, a threat model ought to include profiling of possible attackers and likely attack vectors.

Moreover, multiple threats ought to be carefully considered (see Figure 2), bearing in mind that the cyber dimension is transversal and cross-functional: Every type of threat has often a direct or indirect connection with the cyber domain.

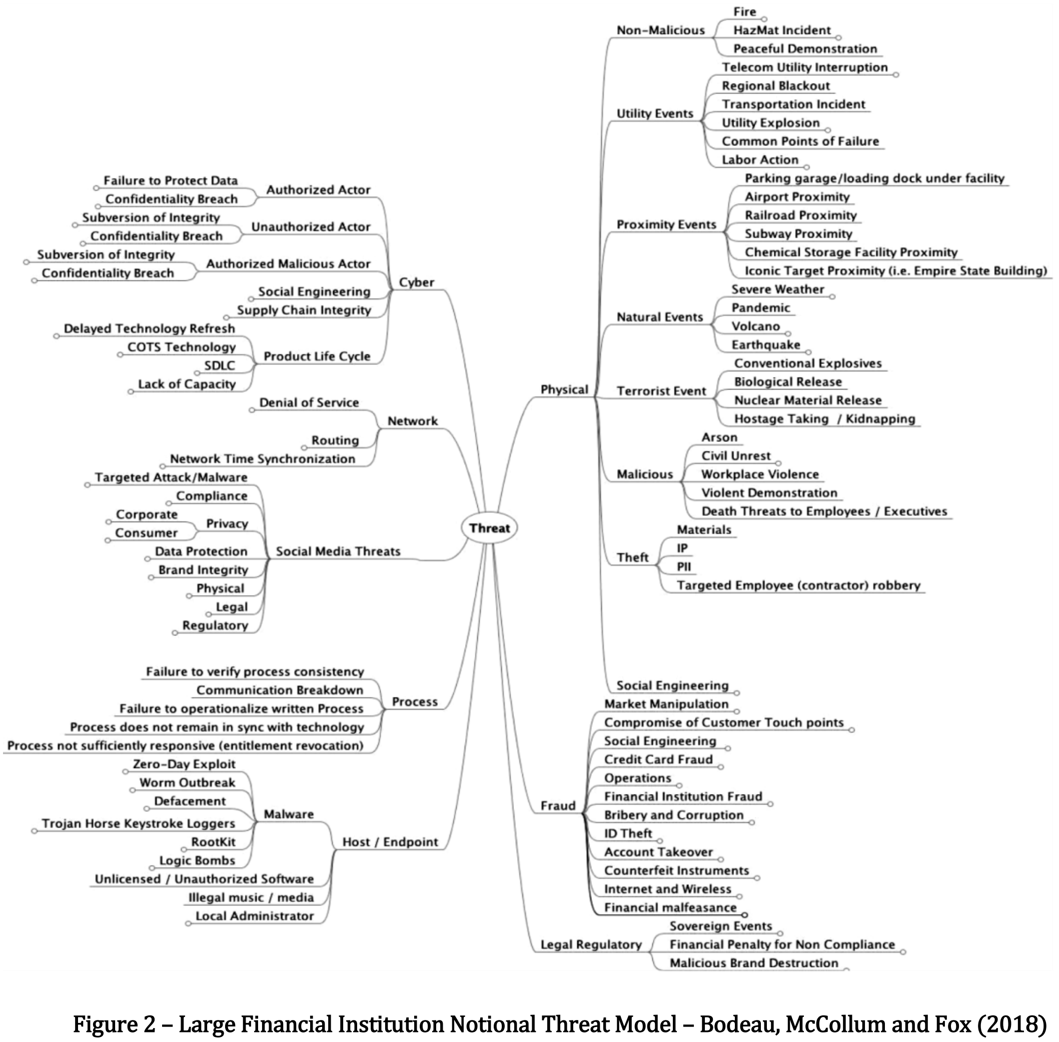


Figure 2 – Large Financial Institution Notional Threat Model – Bodeau, McCollum and Fox (2018)

Besides, central banks are characterized by a large attack surface and by a structured business and IT environment.

With reference to current threat actors and threats, beyond APTs and possible state-backed covert operations, criminal cybergangs and botmasters develop financial malwares, by continually evolving their codes, so as to make intrusion detection and prevention (IDP) more difficult.

IDP is increasingly put to the test by zero-day attacks. Zero-day vulnerabilities are more and more exploited by cybercriminals.[17]

Nevertheless, financial organizations are also affected by a bulk of simple and not very refined cyber-attacks, not to be underestimated as to potential effects.[18]

Phishing, for example, is a simple but very frequent form of cyber-attack. It consists in an attempt to obtain sensitive information, usually by impersonation.[19]

A very sneaky kind of phishing, especially for financial institutions, is "spear phishing": In this case, attacks are targeted and directed towards specific individuals (e.g. "whale phishing attacks", conducted against a CEO or senior executives).

These cyber-attacks are sometimes linked with other types of constantly growing attacks, such as BEC (business email compromise)/CEO fraud. As to the latter, cyber criminals pretend to be a CEO or a senior executive, by spoofing calls, emails and credentials.

All these kind of attacks are carried out by individuals, criminal groups, organized cyber galaxies or they can even be part of more advanced state intrusion campaigns.

Central banks - due to the activities to which they are deputed - are particularly targeted by cyber-attacks aimed at cyber espionage.[20]

This kind of activity can be very insidious for financial institutions: Real espionage motivations can be often masked behind a flaunted theft intent or an apparently failed attack.

As a matter of fact, the main objective of cybergangs and (especially state-backed) APTs is exfiltration – and in some cases, manipulation[21] - of strategic financial data, although purposes are usually multifarious and attack vectors are multiple.

Besides cyber espionage, in the financial sector in general there can be attacks against assets (for instance, theft of money and goods)[22], reputation (e.g. by targeting people and brand) and tasks (for example, for purposes of service interruption).

[17] A zero-day is a computer/software vulnerability with no (known) patches. An exploit directed towards a zero-day vulnerability is called a zero-day attack. Besides APTs, the main criminal cyber galaxies currently active in the financial sector are Ursnif/Gozi/ISFB/Dreambot, Zeus, Carbanak/Cobalt/Anunak/Fin7, Dridex, TrickBot, Emotet, GootKit, Ramnit, Qakbot, Qadars, Baldr.

[18] For instance, phishing, DDoS (Distributed Denial of Service), ransomwares, cross-site scripting (XSS), SQL (Structured Query Language) injection.

[19] Impersonation is the act of pretending to be another person/entity for fraud/exfiltration/espionage purposes.

[20] Cyber espionage can be defined as the activity aimed at exfiltrating sensitive, proprietary or classified data/information.

[21] These attempts could have impact on confidentiality, integrity and availability (CIA parameters) of data. An advanced example of data manipulation is called "data poisoning": This technique allows attackers to influence training data so as to manipulate machine learning results.

[22] In these including crimes related to cryptocurrencies and blockchain.

In this regard, the most fearsome attacks target critical and strategic infrastructures, with possible breakdowns of financial platforms.

Attackers are increasingly employing advanced capabilities, to target core payment systems, transaction platforms and interbank networks.

The evolution of attack patterns, changes in defense capabilities and variations in geopolitical scenarios could modify the geolocation of the current main trends (see Figure 3). In any case, cyber events against financial institutions will continue to be a significant part of all global-scale attacks.

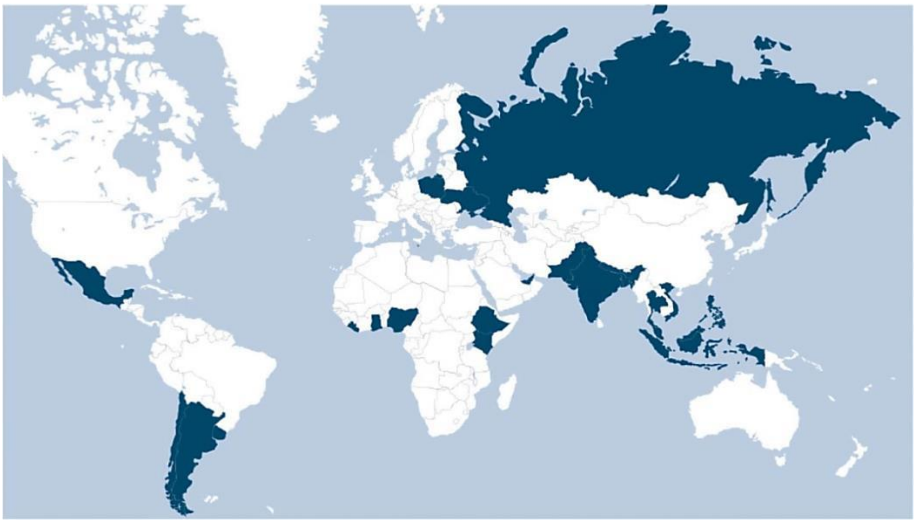


Figure 3 – Geolocations of Payment System Attacks, 2016-2018 – (Nish and Naumann - 2019)

These events, from the simplest to the most structured ones, show a growing disruptive potential: They could be part of covert geopolitical campaigns, hybrid confrontation and asymmetric economic warfare.

A disruption of payment and settlement services can significantly impact the functioning of financial markets. Platforms and systems run by a central bank are vital for the smooth functioning of the financial system as a whole.

3. Development of a cyber threat intelligence apparatus

Considering the intrinsic (structured, meta-polymorphic and targeted) nature of current cyber-attacks directed against financial institutions - it is necessary to use new tools to ensure an adequate protection of strategic infrastructures/information and a resilient reaction towards cyber events.

In this regard, the development of a cyber threat intelligence system could definitely serve the purpose.

3.1 Definitions, Taxonomy and Maturity Model

CTI is a fairly new and elusive concept. In brief, CTI is the activity of collecting, processing, integrating, analyzing raw data about cyber threats and threat actors, in order to provide actionable information to decision makers.

With regard to the three words forming the acronym "CTI", the word "intelligence" (INT) derives from the ancient Latin *intelligentia*, in turn, originating from *intelligĕre* (to understand): It could be defined as *"information that has been collected, integrated, evaluated, analyzed, and interpreted"*.[23]

With reference to the term "threat", it refers, generally speaking, to the possible occurrence of an imminent danger or damage (about to be provoked or about to happen).

The word "cyber" derives from the English cybernetics, which, in turn, originates from the (ancient) Greek root *κυβερ-*.[24] Nowadays, the word cyber refers, by and large, to the virtual world of Information Technology, the Internet and computers.

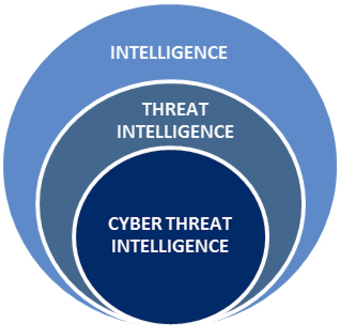


Figure 4 – CTI ⊆ Threat Intelligence ⊆ Intelligence

In line with the above, cyber threat intelligence can be considered, both semantically and practically, as a subset of threat intelligence, which in turn constitutes a subset of the intelligence domain (as shown in Figure 4).

In the CTI field, the term cyber refers to threats: It marks out attackers and means used to conduct attacks, by considering, at the same time, the environment (cyberspace) within which the information is collected.[25]

As far as CTI activities are concerned, they are usually carried out by CERT (Computer Emergency Response Teams) or CSIRT (Computer Security Incident Response Teams). These units perform both CTI tactical activities and CTI strategic activities.

[23] See the World Factbook 2019. Washington, DC: Central Intelligence Agency, 2019 - https://www.cia.gov/library/publications/the-world-factbook/index.html.

[24] There is a parallelism with the Latin root *guber-*, from which originates *gubernator*, helmsman; as to "cybernetics", it derives from the ancient Greek locution *κυβερνητική τέχνη*, *id est* art of the pilot or helmsman (also figuratively).

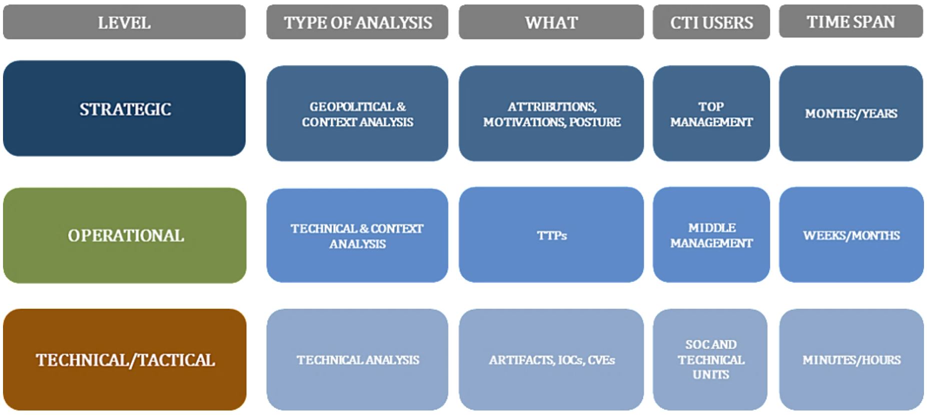
[25] With reference to "cyberspace", there is no fully agreed official definition: The meaning is linked to the online world of computer networks and especially the Internet. More specifically, cyberspace could be defined as the global interdependent network of information technology infrastructures, including the Internet.

CTI's analysts are devoted to technical examination of *modus operandi* employed by threat actors, along with context analysis on trends, connections of cyber events and attributions.

Accordingly, CTI is typically grouped in three main categories: technical/tactical, operational and strategic (for details, see the following CTI taxonomy matrix - Figure 6).

Technical and tactical CTI are usually merged and focused on analysis of artifacts, IOCs (indicators of compromise) and CVEs (common vulnerabilities and exposures)[26].

Through operational CTI, analysts parse TTPs (tactics, techniques and procedures) employed by threat actors.



LEVEL	TYPE OF ANALYSIS	WHAT	CTI USERS	TIME SPAN
STRATEGIC	GEOPOLITICAL & CONTEXT ANALYSIS	ATTRIBUTIONS, MOTIVATIONS, POSTURE	TOP MANAGEMENT	MONTHS/YEARS
OPERATIONAL	TECHNICAL & CONTEXT ANALYSIS	TTPs	MIDDLE MANAGEMENT	WEEKS/MONTHS
TECHNICAL/TACTICAL	TECHNICAL ANALYSIS	ARTIFACTS, IOCs, CVEs	SOC AND TECHNICAL UNITS	MINUTES/HOURS

Figure 5 – CTI Taxonomy with detail of CTI Levels and Types of Analysis

Strategic CTI aims at examining attributions to threat actors, investigating real motivations and links between cyber events, fathoming complex systems dynamics and trends. Geopolitical and context analysis is a fundamental tool.

The maturity model of a CTI system usually includes four classes: initial, managed, repeatable and optimized (as shown in Figure 6).

In a maturity model, elements tend sometimes to overlap: Some features of a higher or lower layer may occur when a given CTI system is at specific level. To set the appropriate rank, a principle of prevalence of the main characteristics must therefore be applied.

At the initial stage, CTI activities are quite informal and a team (e.g. a CERT) operates in a reactive and sporadically proactive manner. There are scarce resources and activities are mainly based on the sole analysts' skills. Knowledge about threats and threat actors is little. The analysis is focused on technical and tactical aspects. Infosharing is limited and community is small. CTI is rudimentary.

At a managed level, raw data and information from internal and external sources are collected and somehow enriched with internal analysis. A threat model, a CTI process and

[26] In digital forensics, an IOC is an intrusion artifact, such as virus signatures, IP addresses and hashes of a malware or domain names of command & control servers (C&C or C2). A CVE is a nomenclature of security-related software flaws.

procedures are defined. The analysis is focused on technical, tactical and operational aspects. Geopolitical and context analysis is episodic. Infosharing begins to take shape, with data and information exchanged through open source platforms, collective fora and peer-to-peer agreements. Threat intelligence platforms or other forms of automation (in these including artificial intelligence – AI) could be introduced. CTI is still basic.

At the repeatable level, CTI cycle and procedures are smooth. The CTI output is aligned with the requirements set by the management. Recommendations and course of actions (CoA) are produced. The analysis is focused on technical, tactical, operational and strategic aspects. Geopolitical and context analysis on threat actors, motivations, capabilities and behavior of adversaries is conducted on a continuous basis. CTI is integrated automatically into preexisting systems and processes. A threat intelligence platform or other forms of automation are definitely introduced. CTI is advanced.

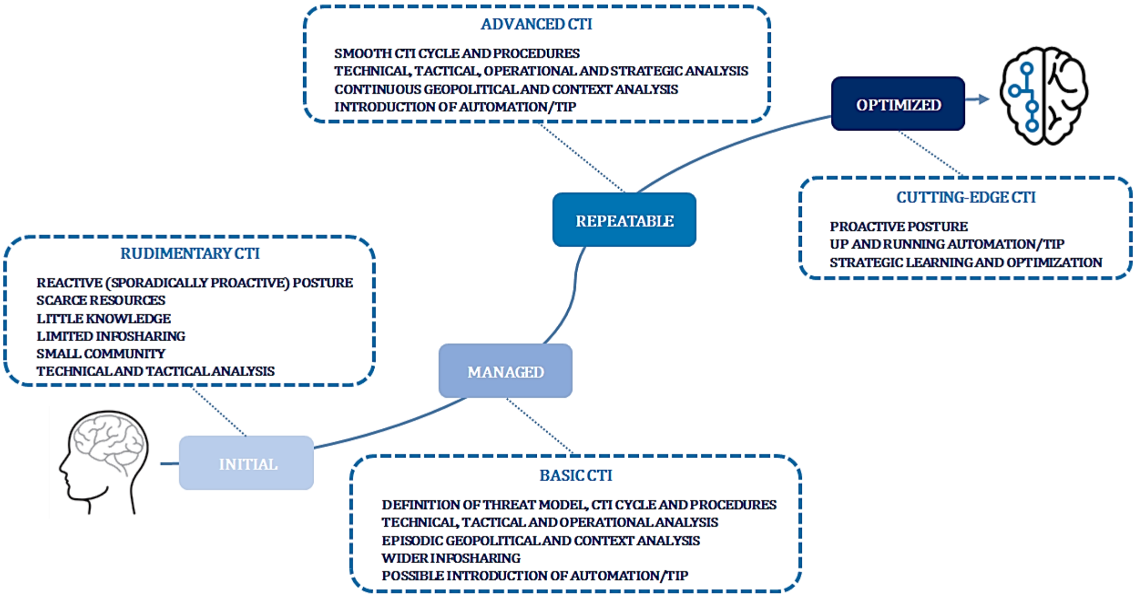

ADVANCED CTI
SMOOTH CTI CYCLE AND PROCEDURES
TECHNICAL, TACTICAL, OPERATIONAL AND STRATEGIC ANALYSIS
CONTINUOUS GEOPOLITICAL AND CONTEXT ANALYSIS
INTRODUCTION OF AUTOMATION/TIP
OPTIMIZED
REPEATABLE
CUTTING-EDGE CTI
PROACTIVE POSTURE
UP AND RUNNING AUTOMATION/TIP
STRATEGIC LEARNING AND OPTIMIZATION
RUDIMENTARY CTI
REACTIVE (SPORADICALLY PROACTIVE) POSTURE
SCARCE RESOURCES
LITTLE KNOWLEDGE
LIMITED INFOSHARING
SMALL COMMUNITY
TECHNICAL AND TACTICAL ANALYSIS
MANAGED
INITIAL
BASIC CTI
DEFINITION OF THREAT MODEL, CTI CYCLE AND PROCEDURES
TECHNICAL, TACTICAL AND OPERATIONAL ANALYSIS
EPISODIC GEOPOLITICAL AND CONTEXT ANALYSIS
WIDER INFOSHARING
POSSIBLE INTRODUCTION OF AUTOMATION/TIP

Figure 6 – CTI Maturity Model

The optimized level refers to a mature CTI status. A threat intelligence platform or other forms of automation are up and running. The main focus is on strategic learning and optimization. CTI is cutting-edge and it is regularly used for decision-making and action.

3.2 CTI Apparatus

The CTI apparatus proposed in this paper was specifically devised for a central bank. The pillars of such a system rest on protection of strategic data and defense of critical infrastructures supporting financial platforms.

This CTI system aims at preventing cyber-attacks launched by different types of threat actors, in particular by those who use financial malwares and rootkits or conduct cyber espionage and interference campaigns.[27] These elements are intrinsically connected to the activity of a central bank, even if one here considers an ever evolving threat model.

The development of a CTI system cannot disregard the definition of rules, procedures and tasks. First of all, it is necessary to outline an internal *ad hoc* process. The devised CTI process can be activated by an internal or external trigger, by requested or received information.

In this phase, information sharing ("infosharing") with community (external CTI user base) counterparts - in accordance with pre-established protocols (e.g. TLP – traffic light protocol) and *ad hoc* conventions - is fundamental.

Infosharing indicates an exchange of information. In such an exchange, sharing patterns are usually framed as follows: One-to-one, one-to-many, many-to-many and many-to-one. As to the one-to-one model, peer-to-peer agreements are preferable, when possible, for guaranteeing a level playing field and regulatory symmetry.[28]

Between CERTs, infosharing mainly concerns news on vulnerabilities and exposures (CVEs), indicators of compromise (IOCs), tactics, tools and procedures (TTPs) of attackers, IP addresses, emails, computer incidents, attributions to threat actors.

When drafting protocols with operating procedures, subsequent to infosharing agreements, it is necessary to consider mandatory standards established at national and international level to analyze and share intelligence (e.g. in some countries, STIX and TAXII).

Since some information and evidence are at the sole disposal of intelligence and law enforcement agencies, there is a need, especially for financial institutions, to strengthen cooperation with these organizations, by means of *ad hoc* agreements.

The ultimate goal of infosharing and of CTI activities in general is to establish a "*supra-system*" - within which this CTI apparatus is enshrined - composed of a network of information networks (in turn, made up of community peers and partners).

As to CTI activities, in a preliminary triage phase, threats must be assigned a score, weighted on the degree of offensive capability, hostile intent and opportunity of the attacker in relation to the degree of exposure of assets (Figure 7).

This score (degree of severity, e.g. category 1, category 2 and so on) could be subject to re-modulation, following the acquisition of new evidence and changing conditions.

[27] A malware (crasis from malicious software) can take the form of executable code, scripts, active content. The code could be for instance a computer virus, a worm, a Trojan horse, a backdoor, a ransomware, a spyware, an adware, a rootkit.

[28] Even if counterparties have a smaller information base and less powerful information systems, their information can prove decisive.

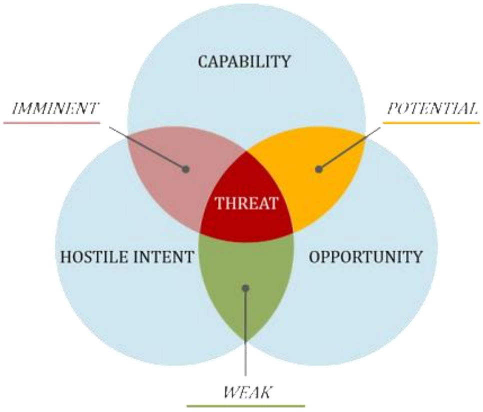


Figure 7 – Qualitative/Quantitative Analysis of Threats: Features and Extent

The ultimate goal - which goes beyond the single case study - of a CTI apparatus is the production of "*sedimented knowledge*", a knowledge base from which to draw for subsequent events or for the development of context analysis: For this purpose, it is essential to adopt a multidisciplinary approach and employ assorted skills.

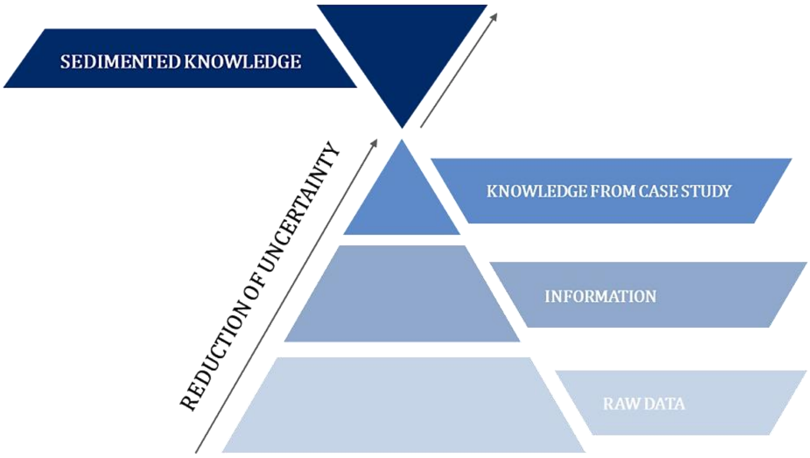


Figure 8 – CTI Reduction of Uncertainty: From Raw Data to Sedimented Knowledge

This sort of sedimented knowledge cannot eliminate the degree of uncertainty relating to cyber threats (Figure 8), but it aims to improve the observation method and to increase the knowledge of phenomena, so as to ensure greater prevention and systemic reaction. [29]

Starting from the prior (sedimented) knowledge of a threat, one could for instance aim at defining the probability of occurrence of cyber events related to it (e.g. through conditional probability or other stochastic methods).

The complexity of the cyber phenomena (understood as the quantity and variety of non-linear relationships between the individual components that constitute the cyber

[29] According to the aforementioned multidisciplinary approach, one here duly takes into account relevant connections with topics such as uncertainty about initial conditions in complex deterministic systems or quantum uncertainty in quantum mechanics.

domain), requires the development of an adequate CTI system, which interacts adaptively with the external environment.[30]

The proposed apparatus – to be considered as a part of the above mentioned "supra-system" - includes a CTI cycle (triggered case by case), a TIP, analysis tools and a set of "*enabling capabilities*" (that operate on a continuous basis) with "sedimented knowledge" (see Figure 9).

The cycle, which originates from the classic intelligence process, is implemented in an iterative way, until the requested output is reached.

The CTI cycle consists of several steps and is triggered autonomously or after a request for information (RFI) received from constituency, third parties of community (peers) or governmental bodies.

The cycle starts with "Planning", a phase in which information gaps are identified and compared with the available knowledge base. For each information gap, a clear search strategy must be defined (TIP, OSINT, infosharing *et cetera*).

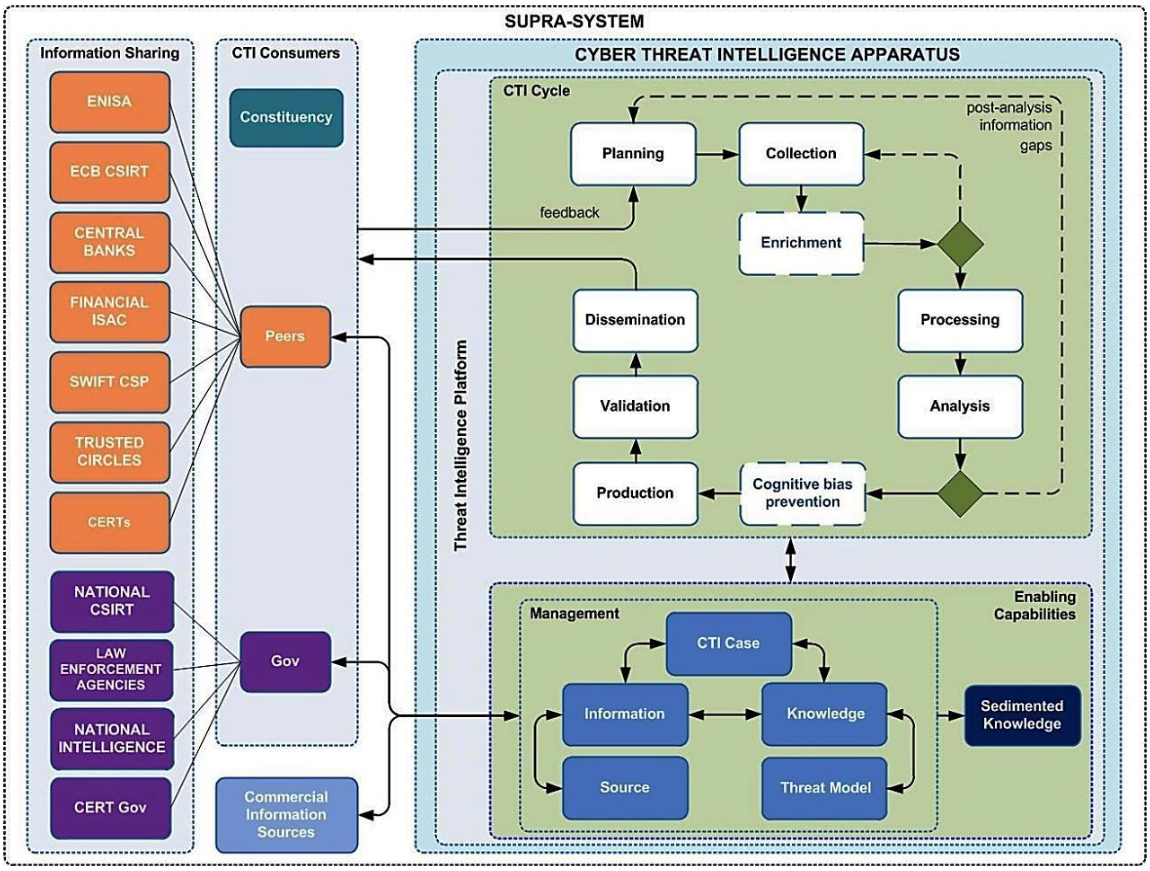


Figure 9 – CTI Apparatus with Detail of Supra-System, CTI Cycle and Enabling Capabilities

[30] The drivers of such adaptation – e.g. mutation and self-organization (in line with *Complex Adaptive Systems* – CAS theory) - ought to be constantly stimulated. According to a swarm intelligence model, the main objective is to spur a collective and adaptive emergent behavior.

Afterwards, the "Collection" phase begins: In this stage, data already available in the knowledge base are merged with new data. With regard to information gathering, it is preferable to adopt an *all-source intelligence* approach.

This phase aims at finding raw data/information from various sources: Web and media (through OSINT, WEBINT, CYBINT), information sharing ("infosharing" with institutional/governmental sources, community, constituency), commercial sources (f.i. threat feeds services); with additional possible forms of external collection (in particular, HUMINT and SIGINT).[31]

The "Processing" step involves standardization of collected data in a common format, with application of ontologies and taxonomies, in order to normalize information coming from different sources.

"Analysis" is a decisive phase. Analysts pull out refined information from raw data, by connecting technical evidence and correlating weak context signals ("connecting the dots").

For the technical analysis of possible intrusions, it is useful to have recourse to structured frameworks.[32] A course of action matrix is effective for identification, prioritization and synoptic representation of actions to be taken.[33]

In the analysis phase, some snags can occur, with onset for example of cognitive biases. Cognitive biases are errors of assessment and judgement induced by simplification strategies and rules of thumb, which arise from the difficulty of understanding.

In order to cope with these difficulties, in addition to the use of structured analytic techniques (SAT), it is useful to define an *ad hoc* process and bespoke rules, without neglecting a multidisciplinary and syncretic approach for multilevel analysis (by employing professionals with various backgrounds).

Accordingly, technical analysis such as DFIR (digital forensics and incident response) and malware analysis must be accompanied by context analysis. In this regard, cyber intelligence (CYBINT – different from cyber threat intelligence) is helpful for this type of investigation.

CYBINT originates from the classical declination of intelligence activities (INTs), with reference to cyber information research. This discipline evolves to include strategic analysis

[31] These types of information gathering are available to law enforcement and intelligence agencies. All the "INTs" could be grouped under the locution "intelligence activities": They differ in the collection method (e.g. OSINT refers to open source intelligence, HUMINT to human intelligence, SIGINT to signals intelligence and so on). As to CYBINT, see *passim*.

[32] For instance, Cyber Kill Chain (Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, Actions) and Diamond Model (Adversary, Infrastructure, Victim, Capability). Further useful analysis tools are MITRE ATT&CK and VERIS.

[33] The course of action (CoA) matrix is made up of two passive actions - Discover and Detect - and five active actions - Deny, Disrupt, Degrade, Deceive, Destroy.

activities and context analysis on trends, geopolitical scenarios and forecasts. These activities pertain to the so-called CTI multilevel analysis.[34]

Some advanced tools of CTI's multilevel analysis are: behavioral pattern analysis, Bayesian statistical models, graph theory and network science, APT galaxies clustering.

With regard to the latter, APTs should be monitored and analyzed on a continuous basis: A non-stop check on plausibility of the attributions and on evolving TTPs is always required.

APT clustering is useful to monitor nation-state galaxies and analyzing possible attack directions, by focusing on data and campaigns grouped by geographical area and sector.

This approach can highlight, for example, real connections between CNOs (Computer Network Operations) and state entities, convergence of different attackers on same targets and sub-targets, recurrences of cyber events.

With reference to graph theory and network science, an in-depth study of interconnections, edges, nodes and sub-nodes could lead the analyst through similar paths of attack or help in tracing threat actors links. Information inferable from such representations could provide concrete indications on actions to be taken.

As to behavioral pattern analysis, automation modeling and Bayesian statistical models, they can aid not only in predictive analysis, but also in threat modeling and validation of multiple informative sources.

In a mature model, CTI should be also complemented by cyber counterintelligence activities, to counter - and where appropriate to continuously exploit - CTI activities carried out by the attackers.[35]

As far as counter-attack or "hacking back" activities are concerned, they could complement a mere neutralization step: However, these actions are not always legally viable and allowed. In case such “active defense” activities comply with the limits established by law, they ought to be conducted, as much as possible, simultaneously to the reaction.

The CTI cycle concludes with: "Production" of a CTI report or an information note (slant of editing - tactical/operational/strategic – and timing depend on type of CTI user); "Validation", that is an analytic approval of the CTI report by a steering manager; "Dissemination", that is delivery of the generated output (“actionable intelligence”) to stakeholders (including governance bodies).

[34] CTI analysis can be descriptive, predictive, prescriptive.

[35] Cyber counterintelligence can be defined as the activity aimed to prevent, detect, contain, counter and eventually exploit cyber intelligence initiatives, conducted by foreign states and foreign intelligence or by individuals and groups.

These three final steps entails effective communication skills. Communication is important for translating intelligence into action. This stage is often critical, due to the possible mismatch between intelligence analyst approach and management needs: In-depth analysis and technicalities must be condensed in concise and clear reports.

As regards dissemination to top management, strategic reports ought to be developed after cyclical research periods, on the basis of context analysis and acquired sedimented knowledge.

After the dissemination phase, a feedback from recipients is essential for the ongoing activity and for subsequent case studies, so as to boost a continuous improvement in the CTI process.

In this regard, the CTI cycle can be reactivated from a previous analysis, in a recursive way. This reactivation can be spurred both by recipients through feedbacks and by analysts/managers at the completion of a first round of the cycle. In both cases, analysts evaluate the adherence of the results of the analysis with the information target required and assess anew variables linked with targeting, sources and threat model.

Depending on the peculiarities of a specific case study, there could be a compression of the CTI cycle, with selected phases and a shortened process.

CTI activities can be supported and enhanced through the use of specific technological tools, for instance by means of threat intelligence platforms (TIPs).

TIPs are aimed at supporting the analysts' activity: They are a useful for correlating and examining threat data, aggregating raw information from multiple sources and automating some steps of the CTI cycle.

TIPs – through automation, integration, standardization, correlation and collaboration – could rise the effectiveness of the generated intelligence, in terms of timeliness, relevance and accuracy.

In particular, TIPs are used for collecting, enriching and merging internal and external data. These platforms help to group and classify a large amount of raw information coming from multiple (internal/external) sources, even in the presence of unstructured data, heterogeneous formats and ontologies.

Thus, TIPs allow normalization of raw information and construction of common models and taxonomies. Furthermore, they can be integrated with existing security systems (e.g. SIEM – security information and event management), through a bidirectional flow of information and signals. TIPs provide support in the analysis phase too: Results should be in any case validated by analysts.

In this regard, during the implementation of a CTI programme, it is necessary to ponder over an adequate and efficient use of automation (and possible AI) tools, so as to obtain maximum advantage and strike the right balance in the human-machine relationship. At any rate, with reference to the decisional and strategic phase, human element ought to be preferred.

4. Implications

Cyber-attacks against a central bank could be aimed at achieving a number of goals. Among the main purposes there are theft, damage to reputation, exfiltration or manipulation of strategic data and, generally speaking, cyber-espionage. However, with a view to a worst case scenario, the most sensitive targets are represented by critical infrastructures supporting financial platforms.

In order to address these attacks, a CTI apparatus has been defined. The implementation of such system can give rise to organizational and systemic implications.

4.1 Organizational Implications

From the development of a CTI system within a central bank, organizational implications can arise: There can be undoubted advantages, but also unfavorable consequences that must be properly considered and, if necessary, mitigated.

It is therefore appropriate to provide a brief overview of the main organizational pros and cons, arising from the introduction of a CTI apparatus in a central bank.

Among the pros, the direct consequence deriving from the introduction of a CTI system can be an increase in capacity of prevention and coordinated management of cyber-attacks.

A certain plus is given by automation, in particular for activities of collection, taxonomy, correlation and analysis of raw data. Furthermore, there may be a leverage effect for technologies related to TIP and a rise in technical skills, both for employees committed with the platform and for IT staff employed in other activities.

In addition, a virtuous side effect is represented by a possible improvement of some business processes, resulting from preventive and rapid resolution of cyber-related glitches.

All these benefits can be reaped in the long term (at least a decade) and are subject to a rigorous implementation of the developed CTI apparatus. An organization could also encounter cyclic CTI failures; ineffective actions and measures does not necessarily mean that the theoretical premises (the CTI apparatus) from which they derive are wrong or to be changed: This may simply depend on a bad implementation. Hence, implementation is as crucial as the principles and requirements it stems from.

CTI technological innovation and skill advancements create opportunities, including greater efficiency and better threat management, but it entails also possible cons.

Amid the potential negative aspects (that could occur in the medium-long term), there may be excessive burden for managing new technologies: This management is a time-spending and expensive activity, which must be well modulated.

Aiming at controlling adverse cost inefficiencies of new IT platforms and technologies (especially when it comes to CTI), the operating costs for the chosen technology should be limited by selecting lean solutions, limiting upstream services on demand[36] and opting for tailor-made platforms (preferably on premise, especially for the processing of confidential data).

Moreover, the introduction of CTI technologies could generate lock-in phenomena[37]. In the presence of non-fungible assets[38] (this is often the case for cyber threat intelligence tools), with regard to IT procurement, it is preferable to announce a public tender/call for bids or to single out services from state-run ad hoc platforms. In any case, an organization ought to work in a transparent manner and with short-medium term contracts (while carefully considering CTI peculiarities and requirements) to avoid information asymmetries, restriction of competition and possible lock-in. A fixed and limited time span could allow to conduct continuous transparent market analysis and to swiftly shift supply of services.

In order to implement a CTI programme, the global measures to put in place are many: A precondition is updating the existing cybersecurity set-up (for instance, by re-organizing cybersecurity roles) and developing new strategic frameworks (e.g. a cyber resilience framework). However, this could lead to discrepancies between internal and external regulation. When developing rules, frameworks and guidelines, an organization/institution must pay attention to avoid possible inconsistencies between internal and external (binding) regulatory environment. A structured organization/institution is usually able to produce rules – at the same time – internally and in national/international fora. In these cases, compliance and consistency between new rules and pre-existing norms should be thoroughly and systematically evaluated (by preemptively applying for instance the principles of primacy and cogency). Furthermore, in order to promote a uniform and coherent regulatory milieu, an organization/institution should strive to encourage regulatory predictability and to reduce regulatory uncertainty, both internally and externally.

In addition, it is worthwhile to dwell upon the relation between automation and human element. As said before, automation can engender benefits. Machines can have a decisive role in the preliminary analysis of raw (big) data; they can also support in the analysis phase. Nevertheless, the human component should remain crucial in strategic analysis and decision-making (as well as in avoiding possible geopolitical interference in

[36] From a business point of view, this stance should be promoted; if not possible, SaaS-like (Software-as-a-service) models are currently preferable.

[37] Lock-in indicates a condition or a period of time during which an organization is not allowed to end or change a financial arrangement.

[38] Non-fungible (nonfungible, unfungible) assets are unique assets, that are not easy to exchange or mix with other assets.

third-parties threat intelligence feeds). Even preliminary phases should be constantly supervised by humans. Analysis and correlation activities performed by machines and platforms are often (but not always) based on preliminary instructions (rules and algorithms set by humans). These instructions could be in some cases non-exhaustive, not applicable or ineffective, thus generating false positive or false negative feedbacks. *Ex ante* and *ex post* human check and evaluation are therefore always needed.

Further organizational problems can derive from a mismatch between CTI operators and business lines or from skills of people employed in intelligence activities.

Timing, procedures and content of CTI (and intelligence) activities may not be familiar or in line with pre-existing habits and customs of business departments. This could create misunderstandings or misalignment. A well-balanced and two-way communication effort is therefore required.

With regard to skills, CTI and INT activities in general require specific behavioral qualities (e.g. as to security protocols, management of confidential information, correct use of electronic devices, restricted access areas, confidential documents, rules of conduct and communication etc.), which go beyond the necessary technical skills. All these abilities can be definitely strengthened through specific training courses.

However, some aptitudes and bents cannot be learned: It appears necessary to *ex ante* evaluate investigative talent, intuition, ingenuity and psychological features of the people to be employed in intelligence activities.

4.2 Systemic Implications

At European level, among the institutional tasks of a central bank, there is the promotion of the regular functioning of the payment system, through the direct management of the main financial circuits. This activity, along with market supervision, aims at backing the stability of the financial system and favoring the effectiveness of the monetary policy.

In this context, corporate and institutional functions are welded together in the systemic implications deriving from the correct and smooth functioning of infrastructures, platforms and market applications run by a central bank (in the European case, these systems are managed - individually or exclusively - under ECB supervision).[39]

A disruption of payment and settlement services can hinder financial markets' operations and liquidity flows.

[39] As far as European financial infrastructures and platforms are concerned, the new Eurosystem single market infrastructure gateway (ESMIG) is intended to provide a unique interface through which users (central banks, commercial banks, central securities depositories) may access T2, T2S, TARGET Instant Payment Settlement and ECMS services offered within the Eurosystem.

Information and payment systems of a central bank are immersed in cyberspace and they are so exposed to a gamut of cyber threats. Potential repercussions for the institution and possible chain transmission effects on the financial sector are momentous.

A breakdown - total or partial, prolonged or temporary - of the main platforms run by a central bank, could produce serious harm to financial transactions and jeopardize the financial ecosystem as a whole. Damages could be both material and immaterial, with impacts on reputation, assets and tasks.

In such a scenario, CTI's preventive activities appear to be crucial, to anticipate cyber threats and to understand their trends: They must be accompanied by systemic and adaptive reaction to adverse events of various kinds - especially cyber events - so as to guarantee a resilient response.

To this end too, CTI activities are key: The locution of British derivation "intelligence-led cyber resilience" appears as effective as it is telling. Accordingly, intelligence activities should lead the way and go along with the development of IT frameworks and architectures, aimed at guaranteeing a cyber resilient ecosystem. Cyber resilience entails an adaptive and prompt reaction: It aims to recover and maintain acceptable levels of service delivery after cyber events, by improving performance, when possible, according to a lessons learned approach.[40]

In this context, on the one hand IT systems and infrastructures, on the other personnel and business processes must be ready to ensure adaptive response and flexible stability. For achieving this goal, adequate, continuous and interactive security awareness campaigns can also be useful.

In any case, among the systemic implications deriving from the introduction of a CTI apparatus within a central bank, one should not only consider those deriving from the protection of critical infrastructures that support financial platforms. CTI serves also to protect the entire spectrum of tasks, activities and reputation of a central bank: From a good or bad prevention of threats directed towards this perimeter, systemic (positive or negative) consequences may derive, on a national and transnational scale.

5. Conclusions

Targeted and meta-polymorphic cyber-attacks against financial institutions are on the rise. This trend could be further fueled by the escalation of asymmetric and hybrid warfare, including potential cyber-attacks directed towards critical financial infrastructures.

[40] A well-balanced cyber resilience strategy provides for resilience goals and means to achieve them, i.e. strategic principles and control requirements. A real measurement of the actual resilience of infrastructures, processes and services and an assessment of the effectiveness of the aforementioned means can only take place *ex post*, when the strategy is put to the test.

Financial institutions and central banks are particularly exposed to cyber-attacks, because of their decisive role in intermediating funds and in managing fundamental financial circuits.

In order to cope with a number of ever more disruptive cyber-attacks, a paradigm shift is needed: From risk management to threat prevention.

Classic cybersecurity tools do not guarantee adequate prevention and detection of structured cyber manoeuvers. Massive cyber-attacks can put a strain on ordinary cybersecurity measures. Classic defensive tools can even be neutralized, if events relate to extensive cyberwarfare operations, destabilization strategies or state interference campaigns.

Cyber-attacks against financial institutions could have several purposes, such as: Exfiltrating or manipulating sensitive and strategic data; stealing money; blemishing reputation; damaging critical infrastructures, including those supporting financial platforms and transnational payment systems.

CTI appears to be a crucial tool for increasing prevention capabilities and resilience, particularly for central banks.

In particular, the development of a CTI system is necessary to cope with cybercrime, hacktivism, cyber espionage, cyberterrorism, nation-state and state-sponsored campaigns.

The intrinsic nature of these phenomena and the peculiarities of the cyber domain, along with the interconnection of diverse interests and threats, require a strategic CTI posture, based on geopolitical analysis, especially in the presence of cyberwarfare and state-backed covert operations.

The introduction of a CTI apparatus in a central bank could bring about pros and cons, both at organizational and systemic level.

With regard to the organizational implications, it is essential to find a sound equilibrium between innovation and stability, in order to avoid internal disarray and misalignment between CTI operators and business lines. It is also key to duly ponder over regulatory, legal, economic, technological and professional consequences deriving from the introduction of a CTI system within a central bank, so as to mitigate organizational imbalances.

As far as systemic implications are concerned, given the high degree of interconnection and the chain reaction effects that characterize the financial system, the introduction of a CTI apparatus within a central bank - by ensuring adaptive reaction to adverse events and enhancing prevention of cyber threats - has the potential to increase the resilience of the financial sector as a whole.

References

Bank of England – Building the UK financial sector's operational resilience – July 2018.

Bank of England - CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations Version 2.0.

Bodeau, McCollum and Fox – Cyber Threat Modeling: Survey, Assessment and Representative Framework – 2018.

Central Intelligence Agency (US) - "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis" Prepared by the US Government (2009), available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf.

Central Intelligence Agency (US) - Richards J. Heuer, Jr. - https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art12.html.

Central Intelligence Agency (US) - The World Factbook 2019. Washington, DC: Central Intelligence Agency, 2019 - https://www.cia.gov/library/publications/the-world-factbook/index.html.

Central Intelligence Agency (US) - The World Factbook 2019. Washington, DC: Central Intelligence Agency, 2019 - https://www.cia.gov/library/publications/the-world-factbook/docs/history.html.

Christine Lagarde – "Estimating Cyber Risk for the Financial Sector" (June 2018).

Christopher Wray – Director of the Federal Bureau of Investigation (FBI) - "Keeping Our Financial Systems Secure: A Whole-of-Society Response" available at https://www.fbi.gov/news/speeches/keeping-our-financial-systems-secure-a-whole-of-society-response - 01 November 2018.

Communication of the Commission Com (2013) 455 final 2013 "Against lock-in: building open ICT systems by making better use of standards in public procurement".

Decreto Presidenza del Consiglio dei Ministri - 17 February 2017.

Digregorio and Giannetto – "Sviluppo di un sistema di *cyber threat intelligence*" – Rapporto Clusit 2019 – February - March 2019.

Dipartimento delle Informazioni per la Sicurezza (DIS) - http://www.sicurezzanazionale.gov.it/sisr.nsf/Relazione-2018.pdf - Relazione sulla Politica dell'Informazione della Sicurezza 2018 – Documento di Sicurezza Nazionale - February 2019.

Directive 2014/18/UE.

Donald C. Daniel and Katerine L. Herbig - Cognitive factors in Deception and Counterdeception, Strategic military deception, Pergamon Press, 1982.

Eleonore Pauwels – "From drone swarms to modified E. Coli: say hello to a new wave of cyberattacks" - United Nations University Centre for Policy Research – 1 May 2019.

Emanuel Kopp, Lincoln Kaffenberger and Christopher Wilson - IMF Working Paper – "Cyber Risk, Market Failures, and Financial Stability" (2017).

ENISA Threat Landscape Report 2018 - 15 Top Cyberthreats and Trends- 28 JANUARY 2019.

Eric M. Hutchins and others - Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains - available at https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

Erica D. Borghard - Protecting Financial Institutions Against Cyber Threats: A National Security Issue - September 2018.

EU Directive 2016/1148 (NIS Directive).

EU Quantum Computing - europa.eu/rapid/press-release_IP-18-6205_en.htm, 29 October 2018.

EU Regulation 2016/679 (GDPR Regulation).

European Commission's Digital Single Market - Policies - https://ec.europa.eu/digital-single-market/en/cyber-security.

FBI - Foreign Influence Task Force (FITF): https://www.fbi.gov/investigate/counterintelligence/foreign-influence.

Federal Reserve System – Information Technology Guidance - https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm.

Financial Cyber Threats (annual) by Kaspersky Lab.

Financial Stability Board (FSB) Cyber Lexicon (12 November 2018).

Financial Times - Cyber attacks on financial services sector rise fivefold in 2018 - 25 February 2019.

FireEye - https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html - March 4 2019.

Framework for Improving Critical Infrastructure Cybersecurity (last version 1.1 released in April 2018) of the National Institute of Standards and Technology (NIST).

Giannetto Boris (and others) – The Review of the ITU's International Telecommunication Regulations: A Threat or an Opportunity for the Internet? – 2012.

Giannetto Boris – Cyber Governance & Cyber Threat Intelligence – Security Summit – Rome 05 June 2019.

G7 Fundamental Elements of Cybersecurity for the Financial Sector (October 2016).

G7 fundamental elements for effective assessment of cybersecurity in the financial sector (June 2018).

GDPR Regulation - Regulation 2016/679/UE.

Governor of the Bank of Italy - 1st Bank of Italy World Bank International Research Workshop - Building Human Capital for 21st Century Jobs – 15 November 2018.

Governor Mark Carney - Bank of England - https://www.reuters.com/article/us-britain-boe-carney-china/china-is-one-of-the-bigger-risks-to-global-economy-boes-carney-idUSKCN1LS0KF - 12 September 2018.

Guidance on cyber resilience for financial market infrastructures of CPMI-IOSCO (June 2016).

http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law:.

http://www.spiegel.de/wirtschaft/unternehmen/huawei-us-behoerden-ermitteln-offenbar-wegen-vorwurf-der-industriespionage-a-1248429.html#ref=rss - US-Behörden ermitteln gegen Huawei – Spionageverdacht - 17 January 2019.

https://www.businessinsider.com/us-asks-allies-to-shun-huawei-china-tech-2018-11?IR=T.

https://www.theaustralian.com.au/national-affairs/national-security/china-used-huawei-to-hack-network-says-secret-report/news-story/510d3b17c2791cbcac18f047c64ab9d8.

https://www.recordedfuture.com/apt10-cyberespionage-campaign/ (February 6 2019).

https://brica.de/alerts/alert/public/1247450/apt-groups-moving-down-the-supply-chain/ (February 14 2019).

https://www.intezer.com/examining-code-reuse-reveals-undiscovered-links-among-north-koreas-malware-families/.

https://www.bankofengland.co.uk/news/2018/november/sector-resilience-exercise

https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

https://www.aljazeera.com/news/2019/02/russian-parliament-approves-bill-isolate-country-internet-190212134228143.html - 12 February 2019).

https://www.us-cert.gov/ncas/current-activity/2017/05/17/ICS-CERT-Releases-WannaCry-Fact-Sheet.

https://csrc.nist.gov/glossary/.

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies;
https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom;
https://www.bloomberg.com/news/articles/2018-10-09/senators-question-super-micro-on-report-of-chinese-hardware-hack.

https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

https://www.ft.com/content/619f9df4-32c2-11e9-bd3a-8b2a211d90d5 (UK says Huawei is manageable risk to 5G – 17 February 2019).

https://www.dhs.gov/news/2018/10/06/statement-dhs-press-secretary-recent-media-reports-potential-supply-chain-compromise, 6 October 2018.

https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology, 30 October 2018.

https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/ - 13 November 2018.

https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018

https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

https://www.ecb.europa.eu/paym/initiatives/cyber-resilience/fmi/html/index.en.html.

https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections.

https://www.ft.com/content/10065056-f8e2-11e8-af46-2022a0b02a6c.

https://www.ft.com/content/34f17e92-fd7c-11e8-ac00-57a2a826423e.

https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

https://ti.360.net/blog/articles/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-en/.

https://brica.de/alerts/alert/public/1247839/apt-c-36-continuous-attacks-targeting-colombian-government-institutions-and-corporations-additional-iocs/).

https://www.wsj.com/articles/washington-asks-allies-to-drop-huawei-1542965105.

https://securityintelligence.com/how-to-defend-with-the-courses-of-action-matrix-and-indicator-lifecycle-management/.

https://www.santafe.edu/.

https://www.us-cert.gov.

https://www.zeit.de/politik/ausland/2019-01/huawei-netz-mobilfunk-spionage-ermittlungen-g5 - Erneut Verdacht der Industriespionage - 17 January 2019.

https://www.ncsc.gov.uk.

https://www.fireeye.com/current-threats/apt-groups.html.

(https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity).

https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/ (February 20, 2019).

https://www.merriam-webster.com/dictionary.

https://en.oxforddictionaries.com.

https://dictionary.cambridge.org/dictionary.

https://csrc.nist.gov/Glossary.

https://csrc.nist.gov/glossary/term/White-Team.

https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

https://www.ncsc.gov.uk/alerts/apt10-continuing-target-uk-organisations.

https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

https://www.group-ib.com/media/cbrf-double-attack/.

https://www.ft.com/content/3662667a-3390-11e9-bb0c-42459962a812 - February 19, 2019.

https://www.ft.com/content/90c07bbe-38ce-11e9-b856-5404d3811663 - “GCHQ chief warns on Huawei security threat” - 25 February 2019.

https://nchoucri.mit.edu/cyberspace-cyberpolitics.

IBM X Force - https://securityintelligence.com/q1-2018-results-gozi-ursnif-takes-larger-piece-of-the-pie-and-distributes-icedid/.

Ilyas Khan "Why you need to quantum-proof your cyber security now" https://www.ft.com/content/9ca0195e-b1c8-11e8-87e0-d84e0d934341 17 October 2018.

IMF Working Paper – Antoine Bouveret - "Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment" (June 2018).

IMF Regional Economic Outlook "Managing the Upswing in Uncertain Times" on Europe (May 2018).

Institute of International Finance (IIF) - Addressing regulatory fragmentation to support a cyber-resilient global financial services industry– April 2018.

Internet organized crime threat assessment (IOCTA – 18 September 2018) by EUROPOL.

Italian Decree 65/2018.

Italian Decree 101/2018.

Italian Public Procurement Code (art. 63).

James Andrew Lewis senior vice president at the Center for Strategic and International Studies in Washington, D.C. – Evaluating a "Cybersecurity Moonshot" - 26 June 2018.

Kalyan Veeramachaneni and others - AI2: Training a big data machine to defend – available at https://people.csail.mit.edu/kalyan/AI2_Paper.pdf.

Keller – "Data and the future of financial services" – WEF – 10 April 2019.

Linee Guida n. 8 of the Italian National Anti-Corruption Authority (ANAC).

McAfee Research - https://www.mcafee.com/enterprise/en-us/about/newsroom/press-releases/press-release.html?news_id=20190303005031 - McAfee Research Gives Rare Look Inside Command and Control of Nation-State Cyber Espionage Campaign – March 3 2019.

MI6 Chief Alex Younger - Secret Intelligence Service, SIS - https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage - 3 December 2018.

Matteo E. Bonfanti - "Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice"– May 2018.

NASA Gobal Climate Change - https://climate.nasa.gov/evidence/.

Nathan Hodge and Mary Ilyushina – CNN World - Putin signs law to create an independent Russian internet – 1 May 2019.

Nathaniel Popper - “Bitcoin Exchange Was a Nexus of Crime, Indictment Says”- The New York Times - 27 July 2017.NATO Wales Summit Declaration - 2014.

NATO Warsaw Summit Communiqué – 2016.

NIS Directive - 2016/1148/UE Directive.

Nish and Naumaan – Carnegie Endowment for International Peace - The Cyber Threat Landscape: Confronting Challenges to the Financial System – March 2019.

OECD Economic Outlook, Issue 1, May 2018.

OECD Interim Economic Outlook, 20 September 2018.

OECD http://www.oecd.org/eco/outlook/economic-outlook/, November 2018.

Office of the Director of National Intelligence - National Counterintelligence and Security Center - Foreign Economic Espionage in Cyberspace – 2018 - https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

Paolo Ciocca and Claudia Biancotti – 23 October 2018 - https://piie.com/blogs/realtime-economic-issues-watch/regulating-data-superpowers-age-ai.

Prof. Alan Turing, "Systems of Logic Based on Ordinals," section 11: The purpose of ordinal logics (1938), published in Proceedings of the London Mathematical Society, series 2, vol. 45 (1939).

Prof. Alan Turing, quotation, from "Intelligent Machinery: A Report by A. M. Turing," (Summer 1948), submitted to the National Physical Laboratory (1948) and published in Key Papers: Cybernetics, ed. C. R. Evans and A. D. J. Robertson (1968) and, in variant form, in Machine Intelligence 5, ed. B. Meltzer and D. Michie (1969).

Prof. Gerardo Beni “From Swarm Intelligence to Swarm Robotics” – in Lecture Notes in Computer Science - 2004.

Prof. Erwin Schrödinger “What is Life?”– 1944.

Prof. Ettore Majorana “The value of Statistical Laws in Physics and in Social Sciences” - 1930s – published posthumous.

Prof. Gu Bin “The Belt and Road Initiative is not China’s Marshall Plan” by - Financial Times 07 August 2018.

Prof. Kevin Werbach - “What the Russia Hack Indictments Reveal About Bitcoin” appeared in The New York Times on 22 July 2018.

Prof. Marco Dorigo and Christian Blum “Ant colony optimization theory: A survey” – in Theoretical Computer Science – 2005.

Prof. Richard Feynman - “Six Easy Pieces” and “Six Not-So-Easy Pieces”.

Prof. Roland Kupers - Resilience in complex organizations - Oxford University – in The Global Risks Report del WEF.

Prof. Thomas Rid and Prof. Peter McBurney - “Cyber-weapons”.

Prof. Thomas Rid & PhD. Ben Buchanan - “Attributing Cyber Attacks” – 2015 – available at https://ridt.co/d/rid-buchanan-attributing-cyber-attacks.pdf.

Prof. Werner Heisenberg – Physics and Philosophy – 1958.

Prof. Yuval Garini and others (Israel's Bar-Ilan University) - Loss of lamin A function increases chromatin dynamics in the nuclear interior” (2015) and “Genome organization in the nucleus: From dynamic measurements to a functional model” (2017).

Prof. Zeng with Stevens and Chen - “China’s Solution to Global Cyber Governance: Unpacking the Domestic Discourse of “Internet Sovereignty”” – June 2017 - (https://www.researchgate.net/profile/Jinghan_Zeng).

Rebekah Brown and Robert M. Lee - The Evolution of Cyber Threat Intelligence (CTI): 2019 SANS CTI Survey – February 2019.

Robert T. Clemen - Making Hard Decisions: An introduction to Decision Analysis, Duxbury Press, Pacific Groove, CA 1996.

Secretary of the Department of Homeland Security Kirstjen M. Nielsen - Speech: https://www.dhs.gov/news/2018/09/05/secretary-nielsen-remarks-rethinking-homeland-security-age-disruption, 5 September 2018.

Senior Deputy Governor of the Bank of Italy Salvatore Rossi - 2° Workshop on Behavioral Financial Regulation and Policy. Opening remarks – 11 December 2018.

Significant Cyber Incidents Since 2006 by the Centre for strategic and International Studies in Washington D.C. - 2019.

Sir Winston Churchill - “Speech at Harvard University, September 6, 1943.

Stratfor - https://worldview.stratfor.com/article/bending-internet-iran-brings-national-information-network-online - 19 June 2018.

SWIFT and BAE SYSTEMS – The Evolving Advanced Cyber Threat to Financial Markets (2018).

Tallinn Manual.

Tallinn Manual 2.0.

TIBER-EU (Threat Intelligence-based Ethical Red Teaming) initiative.

UK Government - HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD - ANNUAL REPORT – 2019 – published on 28 March 2019.

UK Government - Guidance on Exchanging Cyber Threat intelligence – updated 27 March 2019.

United Nations Framework Convention on Climate Change - unfccc.int.

US Department for Homeland Security - "US PRESIDENTIAL POLICY DIRECTIVE/PPD-21".

US National Cyber Strategy – 20 September 2018 – available at https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

US DoD Cyber Strategy – 18 September 2018 – available at https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

William Dixon and Amy Jordan - https://www.weforum.org/agenda/2018/12/why-the-fourth-industrial-revolution-needs-more-arts-graduates/ - World Economic Forum - 11 December 2018.

World Bank Financial Sector's Cybersecurity: A Regulatory Digest (continuously updated)

World Economic Forum - The Global Financial and Monetary System in 2030 – 25 June 2018.

World Economic Forum - The Global Risks Report 2019 – 16 January 2019.

World Economic Forum - The Global Risks Report 2018 – 17 January 2018.

World Economic Outlook 2018 – Cyclical Upswing, Structural Change – International Monetary Fund – April 2018.

World Economic Outlook 2018 – Less Even Expansion, Rising Trade Tensions - Update – July 2018.

World Health Organization - http://www.who.int/news-room/fact-sheets/detail/climate-change-and-health.