Cyber Warning Intelligence:
Enhancing Predictive Capabilities in Cyberspace.
A Comparative Study of the American and Italian Cases

July 2023

University of Glasgow: 2686635S
University of Trento: 233481
Charles University: 722530

Presented in partial fulfilment of the requirements for the Degree of International Master in Security, Intelligence and Strategic Studies

Word count: 24141
Supervisor: Prof. **doc. Dr. Vit Stritecky, M.Phil., Ph.D**.
Date of Submission: 26/07/2023

To my family

Table of Contents

Acknowledgements

The present research project represents the crowning of two years of commitment and sacrifices but also of great satisfaction and indelible moments of joy enjoyed with and thanks to many people who deserve recognition.

I would like to express my profound gratitude to my supervisor, Prof. Dr. Vit Stritecky, who accepted following my research project and who supported its elaboration during the past months with enthusiasm. The passion that he constantly demonstrated in his teachings and in his dialogue with students has consolidated my interest in the interweaving of technology and security and has been a precious source of inspiration. I would also like to thank all my other professors who, with professionalism and dedication, have imparted fundamental knowledge and competences and have been guides for laying the foundations of my future career.

I must thank my University colleagues who became my friends and with whom I shared both my anxieties and laughs and all my other friends who have always made me feel their affection.

Last but not least, special thanks go to my parents who have always encouraged and supported me, my sister who has always wished me luck for my exams (by slipping a card under my bedroom door), my grandparents and my entire family.

Abbreviations

APT	Advanced Persistent Threat
ATT&CK	Adversary Tactics, Techniques and Common Knowledge
AI	Artificial Intelligence
CIA	Central Intelligence Agency
CIOs	Chief Information Officers
CISOs	Chief Information Security Officers
CTOs	Chief Technology Officers
C2	Command and Control
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CIA	Confidentiality, Integrity and Availability
CYBINT	Cyber Intelligence
CO	Cyber Operation
CTI	Cyber Threat Intelligence
CTIIC	Cyber Threat Intelligence Integration Center
CISA	Cybersecurity and Infrastructure Security Agency
DWN	Defence Warning Network Handbook
DPRK	Democratic People's Republic of Korea
DoD	Department of Defense
DDoS	Distributed Denial of Service
EWS	Early Warning System
EDR	Endpoint Detection and Response
IRP	Incident Response Playbook
I&W	Indications and Warning
IoC	Indicator of Compromise

ICT	Information and Communications Technology
ISAC	Information Sharing and Analysis Centre
IT	Information Technology
INSA	Intelligence and National Security Alliance
ITU	International Telecommunication Union
IoT	Internet of Things
IDS	Intrusion Detection System
IPS	Intrusion Prevention Systems
ACN	Italian National Cybersecurity Agency
KPIs	Key Performance Indicators
LAMP	Lockwood Analytical Method for Prediction
ML	Machine Learning
MTTD	Mean Times to Detect
MTTR	Mean Times to Respond
CNAIPIC	National Anti-Crime Computer Centre for the Protection of Critical Infrastructures
CVCN	National Assessment and Certification Centre
NCFs	National Critical Functions
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OT	Operational Technology
PRC	People's Republic of China
PDF	Portable Document Format
PIRs	Priority Intelligence Requirements
SWARM	Scalable Warning and Resilience Model
SRMAs	Sector Risk Management Agencies
SIEM	Security Information and Event Management
SOC	Security Operations Centre
SOAR	Security Orchestration, Automation and Response
SMEs	Small- and Medium-sized Enterprises

SATs	Structured Analytic Techniques
TTPs	Tactics, Techniques and Procedures
TIP	Threat Intelligence Platform
US	United States
USIC	United States Intelligence Community
VA/PT	Vulnerability Assessment and Penetration Testing

Introduction

In recent years, the magnitude, complexity and velocity of threats emanating from cyberspace have been rapidly increasing. The development and pervasive diffusion of information and communications systems have generated novel vulnerabilities that adversarial actors seek to exploit to compromise the confidentiality, integrity and availability (CIA) of the critical data, networks and systems on which public and private organisations rely. In the absence of consensual and/or internationally binding norms governing its functioning and regulating legitimate actions in it, the fifth domain is today a space of confrontation for geopolitical rival states, a source of profit for criminal networks and a forum of activism for hacktivist groups.

In such a rapidly evolving cyber threat ecosystem, malicious techniques are constantly adapting to safeguards and security measures implemented by organisations and, notwithstanding the growing complexity of information systems, their sophistication has often been outpacing theirs. The author of the present research project, therefore, concurs with some scholars, experts and policy-makers in stating the unfeasibility of current measures adopted both in the public and private sectors to secure networks and systems. Organisations' cybersecurity practices are dictated by post-hoc strategies centred around the mission of promptly responding to and recovering from cyber incidents to ensure the continuous delivery of services. Such approach is, however, criticised for its evident inadequacy in limiting the number of successful cyber intrusions and for the significantly rising financial, reputational, legal and other costs in which it results. It is contrarily argued here that organisations must devise and implement more anticipatory strategies and solutions seeking to predict and prevent – rather than merely respond to – cyber emergency events. More

specifically, the present work attempts to address the questions concerning how major public bodies and large- and medium-sized private enterprises might acquire and enhance predictive capabilities in cyberspace by elaborating, applying and integrating within their respective cybersecurity architectures cyber defence early-warning mechanisms. In other words, it intends to investigate cyber predictive best practices and consolidate them within an analytical framework that may support defenders' efforts to thwart cyberattacks before they result in a costly *fait accompli*.

The author acknowledges that cyber phenomena are of difficult predictability. The numerous – both internal and external – variables hindering the ability of organisations' cybersecurity departments to forecast the occurrence and imminence of a certain malicious cyber scenario range from the inherent complexity and obscurity of the fifth domain to the sophistication of technological innovations, from the plurality of strategies and behaviours followed by the equal multitude of (both benign and hostile) players active in cyberspace and again from the regulations adopted to the unintended effects that a given action may trigger (Siciliano, 2022). As a consequence, not all elements of a certain cyberattack scenario can be forecasted. On the other hand, both public and private efforts to gather actionable intelligence with the purpose of predicting and thwarting hostile actions – not necessarily only in cyberspace but more generally in the other operational domains (i.e., air, land, maritime, space) – cannot be expected to result in definite assessments of a certain course of action. The inherent uncertainty of future events and, *a fortiori*, of those in the digital environment does not, however, preclude the possibility to acquire data valuable to anticipate them. More specifically, it has been demonstrated that, in general, it is possible to estimate the typology of cyber operations (COs) that will more probably be employed (i.e., engage in intrusion prediction activities) (Abdlhamed *et al.*, 2017), the ultimate objective behind attackers' motivation to launch cyberattacks (i.e., intention recognition) (Ali Ahmed *et al.*, 2017), the line of action that attackers are likely to follow (i.e., attack projection) (Yang *et*

al., 2014) and the cybersecurity status of defenders' information technology (IT) infrastructure (i.e., network security situation forecasting) (Leau and Manickam, 2015). Over the past decades, numerous have thus been the attempts to elaborate both computational and analytical solutions to precisely and effectively forecast cyber incidents. No definite response has, however, been provided to such a dilemma. The present work will consider Bilyana Lilly et al.'s definition of cyber warning intelligence as "an analytical process focused on collecting and analysing information from a broad array of sources to develop indicators which can facilitate the prediction, early detection and warning of cyber incidents relative to one's information environment" (Lilly *et al.*, 2021) as a reference and will synthetise previous research on the matter to formulate a high-level framework that organisations are recommended to implement for acquiring predictive power in cyberspace. Despite divergent standpoints, scholars, pundits and decision-makers generally maintain that the features of cyberspace offer attackers an edge over defenders (Saltzman, 2013; Lieber, 2014; Shaheen, 2014; Slayton, 2017; Smythe, 2020; Valeriano, 2022b). Whilst not promising to entirely reverse such dynamics, the delineation, formalisation, implementation and integration of a common intelligence-based predictive model within one's extant cybersecurity structure is considered here essential as it allows public and private entities to acquire a more comprehensive understanding of current and future threats and risks to which they are exposed, leverage such actionable intelligence to anticipate potential incidents, reduce the probability of successful digital breaches, develop their capabilities to more promptly halt attacks before significant harms and mitigate their impact, wisely allocate and prioritise investments and resources, as well as to evaluate the effectiveness of the measures adopted (Hutchins *et al.*, 2011). Ultimate outcomes are enhanced preventive capabilities and defensive agility in the fifth domain and, consequently, an equally enhanced cyber maturity.

The issue under investigation here is examined through the comparative analysis of the case studies of the United States (US) and Italy. In reality, true

focal point of the present research project is the Italian case study. The choice of juxtaposing it with the American one is not casual but dictated by two core motivations. Firstly, the author of this work denounces how the debate on both cyber warning intelligence (Caligiuri and Pili, 2021) and other cyber-related matters specifically concerning Italy is still at its infancy, hence the will to contribute to shrinking such a lacuna and to diffusing a vaster understanding of the Italian cybersecurity landscape and of its state of progress. Secondly, the measures adopted by the US, leader in the cybersecurity sector, to protect national networks and systems are analysed and set here as a benchmark for Rome. Widespread is the perception according to which the barriers to entry to the digital arena would be increasingly lowering and numerous new state and non-state actors would be commencing to engage in the fifth domain (Denning, 2009). According to the National Cyber Power Index elaborated by the Belfer Centre of Harvard University, over the past two years, Italy has more actively promoted the cyber defence of its national assets and systems, advancing from the 27th to the 24th position of the ranking. Nevertheless, Rome still lags far behind other advanced economies and the disparity is further accentuated if the level of prioritisation attributed to cyber defence by the US – progressed from the fourth to the third position – is considered (Voo *et al.*, 2020, 2022). By analysing mechanisms to enhance the predictability of cyber threats, this work intends to assess best practices that – on the American model – Rome could implement, errors that it should eschew and shortcomings that it should address to become a cyber power or, at least, to attain an increased level of cyber maturity and security.

The methodology followed for the present work has primarily been centred around a careful analysis of academic articles and books relevant for the study of the issue under examination and published in online databases including JSTOR, EBSCO and IEEE Xplore. Reports issued by renowned cybersecurity private companies and vendors, as well as such primary sources as cyber doctrinal documents and speeches delivered by representatives of the

Italian and American governments made publicly available have also been consulted. The information gathered from such a systematic literature review has been studied in its independence and subsequently employed as a measuring instrument to compare the Italian and American cases. Considering the high level of secrecy inherent in intelligence affairs and the lack of literature on the matter (especially in the Italian case), the absence of more recent and practical insights that the conduction of interviews with experts in the cybersecurity communities of the two country case studies would have allowed to acquire, as well as the focus here solely on major organisations, the scope, depth and detail of the analysis will, however, be limited. As a result, this research project should be conceived of as a mere starting point to address the issue of cyber warning intelligence.

The present research project is structured as follows. The first chapter outlines recent trends in the fifth domain. The second chapter reviews the most recent literature pertinent to methodologies of cyber prediction and prevention. The third chapter describes the cyber warning intelligence framework that, combining the strengths of those already elaborated and attempting to address some of their weaknesses, is recommended to construct more proactive cyber strategies. The fourth and fifth chapters introduce the chosen case studies respectively by discussing most recent trends in the Italian and American cyber threat ecosystems and by assessing measures implemented by the two countries with the objective of forecasting digital threats. The sixth chapter provides some key suggestions on how to more effectively and efficiently implement the framework proposed. A final section concludes the work by synthetising the major findings and by identifying points for future reflection and deeper investigation of the issue.

Chapter One

Recent Trends in the Fifth Domain

Over the past decades, malicious cyber events have alarmingly increased (Greenberg, 2022; FortiGuard Labs, 2022; PwC, 2023). Advanced technologies permit today to more successfully and timely detect suspicious activity in or through the digital space. Nevertheless, estimating with precision the total number of cyberattacks targeting the networks and systems of an organisation over a certain timescale is, to say the least, problematic. Accurate figures remain unfeasible to obtain. Albeit functional to partly distinguish the magnitude of the phenomenon and to eschew discourses inflating the threat but void of objective foundation, existing statistics may portray an outdated, misleading or erroneous picture of the current cyber threat environment (Maschmeyer et al., 2021). Reports published by cybersecurity private vendors, commonly acknowledged as authoritative resources given the leading role played by the private industry in the sector, may not provide the latest data given the rapidity with which the cyber threat landscape evolves. Moreover, they generally focus on specific categories of cyberattacks, industries and/or regions. Cyber operations (COs) may differ and the alert raised for a certain threat may not equally concern all sectors. Major cybersecurity firms are based in the United States and their Western perspective may lead to an over-representation of American and European organisations in their figures, not necessarily justified by a major frequency of cyberattacks against them or their major vulnerability but by the mere overlooking of other regional areas. An additional issue that questions the reliability of such reports consists in the paucity of transparency in the methodology followed to compose them. Unclear is not only the definition of cyber incident used and thus the requirements that a cyber event needs to fulfil

in order to be included in the dataset, but also the provenance of the data reported (www.cfr.org; www.iiss.org). Finally, it is worth mentioning that a complex interweaving of reputational and strategic considerations often plays here: on the one hand, cybersecurity private vendors are encouraged to inflate the numbers in order to demonstrate their capabilities, attract new clients and raise profits; on the other hand, organisations targeted by malicious COs are discouraged to report incidents in order not to incur in losses of credibility and customers, as well as in legal costs.

Despite confusing numbers, cybersecurity experts, scholars and policy-makers concur in stating the rapid increase of cyberattacks. Yet, malevolent activities in the fifth domain have thus far remained below the threshold of conventional conflict (Rid, 2012, 2013; Brantly *et al.*, 2016). The empirical studies conducted by Ryan C. Maness et al. demonstrate that the daunting prognostics according to which states would engage in a *bellum omnium contra omnes* in cyberspace (Arquilla and Ronfeldt, 1993; Arquilla, 2012a, 2012b, 2013) have not realised. Contrary to such a Hobbesian scenario that dominated the scholarly debate (Langø, 2016) in the 1990s, cyber incidents have been primarily involving regional rival state actors seeking a strategic edge over their longstanding adversaries (Maness, 2016). Such pattern has yet not failed to raise concerns. Rivalries are unanimously depicted as potential perilous dynamics for regional and international stability (Goertz and Diehl, 1993; Diehl, 1998) and experts have been preoccupied with the repercussions that their traditional proclivity to escalate into various forms of aggression might have in the current digital age. It has been argued that states tied by enduring relations of antagonism would consider any option at their disposal, even those that might endanger their own security, in order to harm their rivals' interests. Cyber tools are indeed additional assets in a state's arsenal that, if employed – either independently or in conjunction with others – have the potential to cause significant damages. Neighbouring states may thus spread malicious software (malware) into the networks of their rival counterparts and adopt any malevolent

digital technique in the attempt to prevail over the enemy (Valeriano and Maness, 2012). However, as Maness et al. explain, states have thus far demonstrated restraint in their interactions in the digital arena. The authors' empirical evidence reveals that of the 126 couples of rival states identified between 2001 and 2011, only 20 were involved in cyber conflicts. Depending on their correlation or not with other similar episodes, the investigation classifies COs into cyber incidents and cyber disputes. The former are understood as individual malicious cyber actions limited in time and pursued by state entities against adversary states, while the latter are broader cyber campaigns. The study reports 110 cases of cyber incidents within 45 cyber disputes (Maness and Valeriano, 2016; Maness *et al.*, 2017a, 2017b). Two subsequent versions of the dataset have extended the period under examination first to 2014 and later to 2016 and have respectively identified 192 and 266 COs between antagonistic dyads (Maness *et al.*, 2019a, 2019b, forthcoming, Valeriano, 2022a). The research, therefore, confirms that COs conducted by rivals are on the rise. Nonetheless, their numbers continue to remain relatively low.

As per Brandon Valeriano and Ryan C. Maness, states' tendency towards cyber restraint is justifiable by two major reasons. Firstly, even admitting that states had been able to develop the tools necessary to launch serious cyberattacks, they would prefer not to utilise them under conditions of tolerable tensions with a traditional foe out of fear of retaliation from the latter. The reproducibility that often characterises digital instruments allows the target and a multitude of other malicious actors to counterattack and engage in a possibly interminable tit-for-tat dynamic in cyberspace. *A fortiori*, states would shun to trigger (and be considered responsible for) the direst case of a cyberattack against the critical infrastructures of a rival that might result in diffused disruption and cascading effects threatening its national security and interests. Such an incident may, in fact, be qualified by the targeted state similarly to a conventional form of aggression but the party launching the attack might not be

prepared or willing to engage in the vicious cycle of conventional responses (e.g., economic sanctions, armed confrontations) that such an interpretation would legitimise (Hathaway *et al.*, 2012). Secondly, the authors argue that "[t]he rules of the game in cyberspace have yet to be determined *but* states have yet to employ blatant widespread damage via the Web […] *fearing* the unknown or *the disturbance of* the balance of harmony during a rivalry" (emphasis added) (Valeriano and Maness, 2012). Cyberspace is imbued with complexities and uncertainties that might generate unintended effects even from an apparently innocuous CO and that thus deter the use of computer technologies in the first place. States would consider recurring to the fifth domain not with the intent of initiating or reviving a spiralling escalation of tension but with that of signalling their resolve over a certain issue while easing the nervousness with the rival counterpart (Valeriano and Maness, 2012).

Furthermore, for the reasons illustrated above, states have previously appeared restrained not only in their decisions to exercise their cyber power against an enemy target, but also in their choice of the cyber instrument to display in the event that they have opted to launch a cyberattack. Valeriano and Maness have proved that the vast majority of cyber incidents and disputes between adversarial states on record have been espionage operations or have utilised relatively unsophisticated and low-impact techniques (Maness, 2016). Notorious exceptions have surely not been lacking and the case of Stuxnet represents an illustrative instance. In 2010, researchers at the Belarusian Internet security firm VirusBlokAda discovered that the worm had infected the Iranian nuclear power plants in Natanz (Farwell and Rohozinski, 2011; Van Puyvelde and Brantly, 2019, www.trellix.com). The episode attracted the attention of international media and cybersecurity experts, who depicted Stuxnet as "the most menacing malware in history" and "a sophisticated and destructive digital worm" (Zetter, 2011), "a military-grade cyber missile" (Farwell and Rohozinski, 2011; Van Puyvelde and Brantly, 2019) or again as "one of the most sophisticated and unusual pieces of software ever created" (McMillan, 2010).

Altering the speed of the motors of the nuclear centrifuges, the notorious malware, in fact, destroyed about 1,000 of the 4,000–6,000 centrifuges at the time active in Iran and later spread in numerous other countries, causing the malfunctioning of more than 60,000 computers (Van Puyvelde and Brantly, 2019). Iranian government officials accused the US and Israel, who confirmed their involvement only two years later, in 2012. Firstly outlined in 2006, the so-called "Olympic Games" operation was launched by the US National Security Agency (NSA), the Central Intelligence Agency (CIA) and the Israeli intelligence services in 2008 (Nakashima and Warrick, 2012). The computer worm aimed at sabotaging the Iranian uranium enrichment programme but its code was subsequently manipulated to deliver other malware attacks (Duqu, Flame, Havex, Industroyer and Triton) (www.trellix.com). On the other hand, the dark web is a notorious repository of malicious cyber tools vended to the best bidders or freely available (Shahriar *et al.*, 2022). Cicilia Zhang et al. illustrate, nonetheless, how also open-source data may serve the malicious objectives of states and non-state groups in cyberspace. Such data contained in technical reports and demonstration videos of successful intrusions into the systems of critical infrastructures published online by experts and academics, as well as in software programmes, open-source tools, tutorials and various materials designed for ethical hackers and easily downloadable online, constitute a double-edged sword. They may be intended for forensic, educational, transparency or other legitimate purposes but, if coupled with general information available online about critical infrastructures, the functioning of their systems and potential vulnerabilities in them, may assist hackers in the development of malicious cyber tools and attack strategies (Zhang *et al.*, 2022). Such an ease of access online to a plethora of valuable material to instruct in detail on how to deliver malicious codes has contributed to the perception that penetrating networked systems does not require extraordinary technical competences. When considering low-level digital techniques, the argument may indeed hold. Yet, COs differ in procedure,

sophistication, intended objectives and outcomes (Thomas, 2022). Hence, designing and launching such large-scale COs as Stuxnet imply considerable physical, technological, financial and temporal costs that only few states are currently able to sustain.

The restraint that Maness et al. have illustrated as characterising – due to both strategic and technical constraints – inter-state interactions in cyberspace is surely to be welcomed with (a note of) optimism. Nevertheless, concluding that these patterns will remain consistent or going so far as to interpret them as an unquestionable constant is rash and risky and may lead to dramatic surprises. Given the absence of an authoritative and common definition of what is deemed legitimate in or through cyberspace, it cannot be excluded that a certain cyber malicious action or its unintended effects may be judged as requiring a robust response and may thus seriously escalate tensions between the parties. Furthermore, it would not be a novelty if an incautious use of digital assets creates a perilous discrepancy between the intent and the actual harm caused by a cyber event (Bellovin *et al.*, 2017). Finally, even acknowledging its validity, the research by Maness et al. has excluded non-state COs from the analysis and it is not possible to generalise its findings to the various actors active in the digital arena (e.g., nation states, state-backed agents, cyber criminals, hacktivists, individuals). If not financially backed by national or international governments, cyber criminal groups generally lack the resources to launch significant COs. Moreover, the vast majority of their low-level attacks is automatically forestalled by technological instruments and common practices of cyber hygiene. Nonetheless, the authors themselves recognise that non-state players may not restrain their malevolent activities in cyberspace and adopt instead a more unscrupulous behaviour (Maness, 2016). Hackers have been observed launching targeted malware, ransomware, phishing, Distributed Denial of Service (DDoS) and other attacks against high-profile public and private entities and subsequently enlarging the scope of their malicious COs to maximise profits. Given the saturation of the market of cyber criminal tools,

they have continually been adapting and evolving their *modus operandi*, whilst investing into obfuscation-as-a-service capabilities and other technologies with the intent of better concealing their identity in cyberspace and bypassing defence mechanisms (PwC, 2023). Jacopo Bellasio et al. forecast that "[a]dvances in new and emerging technologies are likely to contribute to a continuation and exacerbation of current cybercrime trends and activities". As the authors clarify, "[t]he increasing availability of more powerful, easier to use and less expensive technologies is likely to further stimulate the conduct of cybercrime activities by a wide array of individuals with an interest in making quick financial gains". Moreover, they observe that "the development of new, complex technological solutions and capabilities may enable cybercrime professionals, organised groups and state-sponsored actors to conduct complex attacks and activities, resulting in higher criminal returns and, potentially, nefarious impacts on the stakeholders and individuals targeted" (Bellasio *et al.*, 2020a, 2020b). Artificial Intelligence (AI), Machine Learning (ML), autonomous machines and systems, computing and data storage technologies, telecommunications infrastructures, Internet of Things (IoT) and privacy-enhancing technologies allow to generate, store, access and manipulate data and may, therefore, encourage current and new forms of cybercrime, while ensuring increased anonymity given the equally increased complexity of tracking, attributing and charging perpetrators (ENISA, 2023).

Cyber operations (COs) surely are attractive tools promising state (Brantly, 2014; Brantly *et al.*, 2016) and non-state actors to attain their interests and objectives. Focusing on inter-state dynamics, Max Smeets contends that offensive COs could be key strategic assets for national governments. More specifically, Smeets formulates four propositions that would demonstrate the strategic value of possessing offensive cyber capabilities. Firstly, the author argues that the latter would be an additional option among other (conventional) tools and would thus allow decision-makers a more extensive margin of choice and manoeuvre in their foreign policy. Moreover, the malleability that

distinguishes cyber instruments would allow their use across the entire spectrum of scenarios, from situations of peace to others of conflict. Secondly, offences launched in the digital space may integrate and complement military capabilities, thus allowing to wage an asymmetric warfare against the adversary party and to potentially have a multiplier effect on the kinetic force deployed. Finally, Smeets explains that not only may they be effective in reaching the goal behind their use while limiting casualties and damages, but, by embarrassing, humiliating and degrading their confidence, they can also allow governments to acquire a psychological edge on rival states (Smeets, 2018). Joseph S. Nye succinctly concludes that "cyberspace is a new and important domain of power" for states (but not exclusively) (Nye, 2010). More generally, digital tools are, in fact, described by state and non-state actors as having a strategic utility since they are non-lethal and do not pose significant risks to the physical security of individuals that recur to them, they may allow to attain various interests and purposes while not implying excessive costs and retaining plausible deniability given the difficulties in attribution processes.

Finally, besides following a rapid upward trend, today's COs have attained increased levels of sophistication and impact. As mentioned above, new technologies offer new opportunities of abuse. The development and proliferation of autonomous devices and systems have been enlarging the attack surface and the pool of vulnerabilities that can be exploited by malevolent actors. No cyber incident has thus far been directly related to casualties. Nonetheless, they are often responsible for considerable financial and other costs, not only for the targeted organisation but also for third parties having various degrees of connection with the latter. Phil Williams et al. have long associated today's growing dependence on information and communications systems with the emergence of new vulnerabilities and have warned that "with the expansion and growth of technology, simple dependence is evolving into interdependence". As the authors clarify, "[w]hat happens to one system now has the potential to effect operations on myriad other systems that are only

peripherally related to the target of the initial intrusion" (Williams *et al.*, 2002). The often transborder diffusion of cyber events is particularly problematic as it not only multiplies their impact and costs, but it also complicates the comprehension, countering and, as a consequence, future prediction and prevention of cyber threats.

Chapter Two

Literature Review

In light of the alarming cyber threat environment delineated in the previous chapter, the author of the present work argues that imperative is the formulation and accurate implementation of models, strategies and processes seeking and able to forecast and prevent – and not merely respond to – hostile cyber events before their occurrence. Whilst acknowledging the complexity of the issue and thus the need to eschew monocausal explanations, the proliferation of malevolent COs is, at least in part, both the cause and effect of inexistent or inadequate cybersecurity practices. Bilyana Lilly et al. observe that "[d]espite increased focus on developing more sophisticated cybersecurity tools and techniques for defending organisations against cyber threats […], the cyber defence community is still largely reacting to, rather than predicting or anticipating, these threats" (Lilly *et al.*, 2021). Both public and private organisations have, in fact, traditionally tended to concentrate on the post-intrusion phase of cyberattacks and their cyber incident response schemes are generally better defined in comparison to their – if any – pre-intrusion strategies.

In reality, since the 1990s, the Cold War theory of deterrence has instructed nation states' efforts to avert a "Cyber Pearl Harbour" (Smeets and Soesanto, 2020). Strategies of deterrence by denial (Wenger and Wilner, 2021), punishment, entanglement and delegitimisation have thus variously been adopted over the past decades (Smeets and Soesanto, 2022; Welburn *et al.*, 2023). Nevertheless, academic arguments over their application in the digital space remain contrasting and dubious is their effectiveness. Some scholars contend that cyber deterrence would follow the logics common to conventional

domains and would hence succeed or fail according to, *inter alia*, the active discouragement of adversarial actions, the enlargement of the security perimeter and the establishment of norms and international agreements (Goodman, 2010; Jensen, 2012; Denning, 2015; Lilli, 2021). As an illustration, whilst denouncing Washington's failure to inhibit further malicious behaviour in cyberspace by its traditional rivals due to no or timid and delayed responses to previous attacks, Susan Hennessey does not *in toto* reject the concept of cyber deterrence but rather calls for a more assertive deterrence posture (Hennessey, 2017). On the contrary, other experts assume the peculiarity of cyberspace in comparison to the other domains and claim that cyber deterrence is only possible following a thorough comprehension of the former's operational dynamics (Tor, 2017; Muller and Stevens, 2017; Kello, 2017; Healey, 2017; Nye, 2017; Wilner, 2017). Finally, a third direction along which the debate has been developing argues for the unfeasibility of deterring threat actors' COs (Fischerkeller and Harknett, 2017; Brantly, 2018a). *Conditiones sine qua non* for an effective deterrence strategy are, in fact, the ability to attribute the act considered as meriting retaliation to a specific actor, the establishment of thresholds between acts that may go relatively unpunished and those that may contrarily prompt a fierce response, the targeted state's credibility in its will and alacrity to retaliate, as well as the availability of the resources necessary to enforce that will. Such conditions are, nonetheless, complex to fulfil in cyberspace. As mentioned, attributing a hack to a specific actor is a delicate and complex issue. Diverse arguments have been advanced (Brantly *et al.*, 2016). Nonetheless, cybersecurity scholars and practitioners concur that the intrinsic features of the digital environment (i.e., the latter as being a de-territorialised, transnational, fluid and opaque space), the plurality of the actors active in it and the elevated sophistication of cyber tools thwart the definite attribution of a cyber malevolent event (Kello, 2013). Should the attribution dilemma be resolved, governmental authorities would still have to determine if the particular circumstances require a reaction and, in a positive case, agree in the nature of the latter. Moreover,

retaliation following a cyber incident intends to demonstrate resoluteness but must be proportionate and timely lest it is interpreted as a proper attack. Finally, measures implemented to deter a certain actor may not be effective for the entire plurality of players active in cyberspace (Iasiello, 2014).

Whilst deterrence strategies are increasingly losing traction due to their unsatisfactory performance in reducing the number of cyber events (Soesanto and Smeets, 2021), in recent years, experts have in contrast incessantly stressed the importance of constructing a resilient cybersecurity perimeter (Knake, 2019). Key notion among both governmental bodies and private corporations, cyber resilience is commonly related to the ability of promptly recovering from a digital breach (Linkov and Kott, 2019). The US National Institute of Standards and Technology (NIST) describes it as "the ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs" (NIST, 2011). Other definitions of the concept indicate it as a more holistic approach encompassing activities not only aimed at restoring services following a cyberattack, but also at anticipating and preparing for malicious COs (Galinec and Steingartner, 2017). Such ability is surely essential as it contributes to minimising the impact of a cyber incident. However, merely enhancing resilience is not a sufficient condition for securing critical networks and systems. In recent years, the concept of resilience has informed the manufacturing chain of information and communications technology (ICT) products and services since its earlier stages and significant have thus been the attempts to *ex ante* construct a more robust ecosystem towards adverse cyber events (Björck *et al.*, 2015). Nevertheless, resilience remains a deficient, reactive approach (Herrington and Aldrich, 2013).

As mentioned above, the present research project inserts itself into that line of academic work that considers as imperative the abandonment of such

merely reactionary cybersecurity strategies and the implementation, on the contrary, of warning intelligence methodologies able to lead and support the prediction and prevention of digital breaches. Also referred to as indications and warning (I&W) or indications intelligence, the concept and a first system of warning intelligence were developed in the post-World War II period. Following the 1941 Japanese attack on Pearl Harbour, the United States Intelligence Community (USIC) was concerned with the potential replication of similar attacks against American targets and thus with the urgency of elaborating analytical models for monitoring and preventing adversarial activities or, at least, for anticipating them with timeliness sufficient to adopt mitigating counter-measures (Laur, 1986; Hulnick, 2005). Notwithstanding its criticality, neither the USIC nor Washington's allies have agreed upon a common definition of the notion of warning intelligence. The American Department of Defense (DoD) denotes it as "those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intentions against United States entities, partners or interests" (DoD, 2013b). Other definitions may dissimilarly specify some elements (e.g., the object of the warning) but constant remains the function of threat forecasting and communication to decision-makers.

Various are the I&W frameworks that, over the past decades, have been elaborated within the intelligence, military and academic circles, as well as by public and private research centres and that have been utilised to monitor and predict potential adversarial actions. Their exhaustive revision would be unfeasible here owing to both their numerousness and, in some instances, also due to their confidentiality. The present work thus briefly focuses on the Lockwood Analytical Method for Prediction (LAMP), the Defence Warning Network (DWN) Handbook and on the Seven Phases of the Intelligence-Warning Process. Notwithstanding sharing a similar purpose, such paradigms differ in the level of specificity, the number of phases in which they are articulated, as well as in the emphasis attributed to each of the latter. More

specifically, the LAMP model, whilst acknowledging its fallibility – due, *in primis*, to the fact that future events occur according to a dynamic spectrum of probabilities in continuous change –, is described as a practical structured analytic technique assisting in the forecasting of the probability of a certain scenario at a given time. According to the method, analysts would acquire such anticipatory power following the clear and precise definition of the issue upon which to formulate predictive hypotheses, the determination of the actors involved, the conduction of an extensive study of the perceptions and intentions of each actor over the issue, the specification of any possible course of action, the determination of major scenarios, the calculation of the total number of alternate futures, their pairwise comparison and ranking to establish their relative probabilities, the conduction of an analysis of the alternative futures' possible consequences for the issue in question, the determination of focal events and the compiling of a list of indicators suggesting the occurrence or imminence of a certain event and, finally, the assessment of the potential for transposition between alternate futures (Lockwood, 2002, 2010; Clausen, 2010; Singh, 2013). Similarly, the DWN Handbook states the criticality of structuring the prediction of possible future threats according to scenarios. Developed by the American DoD, the model consists of five stages, namely the identification of anomalies, the advancement of alternative scenarios, the identification of conditions, drivers and indicators for each course of events hypothesised and the determination of their respective warning thresholds, the evaluation of measures adoptable to influence or mitigate the threat in question and the final communication of the warning alert. Nevertheless, contrary to the preceding method, the DWN Handbook has a more policy-oriented approach and, therefore, majorly highlights the importance of timely providing national and defence decision-makers with alerts about a certain threat and the broadest set of possible options to mitigate it (Department of Defense, 2020). Finally, the seven phases of the Intelligence-Warning Process (i.e., the identification of the key elements of information required for the forecasting of a certain issue, the

publication of a plan for the collection of intelligence, the consolidation and classification of information obtained, the drawing of initial conclusions, the latter's refinement and updating according to further data addressing intelligence lacunae and the communication of the analysis' outcomes) aggregate the major aspects of the LAMP and DWN paradigms, thus resulting in a more balanced approach (Lilly *et al.*, 2021).

Over the past decades, the notion and frameworks of indications and warning (I&W) intelligence have been variously stretched and adapted to the evolution of the threat environment. More specifically, in the bipolar period, that of I&W was a practical and frequently-used tool for handling the Soviet Union. In the 1990s and 2000s, the emergence of non-state threats coincided, on the contrary, with the initial overlooking of its techniques. James J. Wirtz observes that what was once a fundamental and verified methodology employed by intelligence analysts to alert military officers and policy-makers about deviations or anomalies in rivals' behaviours and hence about the increased probability of a certain perilous or aggressive act against national targets, in recent years, has been neglected. The author notices that, despite still being praised by eminent intelligence scholars and practitioners, I&W intelligence is predominantly considered as a product developed during the Cold War and solely circumscribable to that specific context. In particular, two are the major motivations generally adduced for its alleged inapplicability to address contemporary threats. Firstly, in comparison with conventional ones, the latter are maintained to not generate signals of sufficient magnitude to be analysed with traditional I&W techniques. Secondly, they would purportedly be characterised by a degree of novelty and unpredictability that precludes their forecasting. Wirtz refutes, however, such line of reasoning claiming that non-state actors not only often have a patterned and hence predictable behaviour but that they are also constrained to follow a certain *modus operandi* due to their scarce resources (Wirtz, 2013). Similarly to Wirtz, the present research work recognises the differences of visibility between conventional and contemporary

menaces and the complexities that such differences introduce for the employment of predictive analytical techniques. Nonetheless, it elaborates on his study by contending that warning intelligence methodologies may serve as a key tool both for governmental agents and private sector entities (e.g., industry, academia) to tackle not only non-state but also cybersecurity threats. Since the 2007 Distributed Denial of Service (DDoS) attack on Ukraine (Lewis, 2023), some scholars and practitioners have, in fact, transposed and adapted them to cyberspace with the objective of proactively anticipating cyberattacks by retrieving and analysing cybersecurity intelligence information. In line with the disagreements over the notion of warning intelligence, no unanimously-accepted definition of the corresponding concept applied to the cyber domain has, however, been elaborated. For the purposes of clarity, Lilly et al.'s definition of cyber warning intelligence as "an analytical process focused on collecting and analysing information from a broad array of sources to develop indicators which can facilitate the prediction, early detection and warning of cyber incidents relative to one's information environment" is here considered as a reference (Lilly *et al.*, 2021).

The concept and paradigms of I&W have been flourishing in other intelligence domains. On the contrary, they both remain at their infancy in the cybersecurity one. The American DoD has correctly stated that "cyberspace I&W may recognise adversary cybe[r] operations (CO) triggers with only a relatively short time available to respond" (DoD, 2013a). The minor physicality and tangibility of the digital domain (Russell, 2017; Martino, 2021), the plurality of users active in it, the enlargement of the attack surface, as well as the development of increasingly sophisticated technologies and malevolent tactics are factors that cripple the effectiveness of cyber indications intelligence models and question their very use. Forecasting events in such a complex, obscure and lawless space as the information domain is undoubtedly far from being straightforward. Yet, predicting adversarial CO – and employing analytical frameworks to do so – has proved to be not only feasible but also

beneficial. Contrary to conventional discourses affirming how they would occur with such a rapidity that impedes their spotting, cyberattacks and, *a fortiori*, sophisticated cyber campaigns perpetrated by state and/or state-backed agents demand a preparatory time that, albeit variable, is often sufficient to allow the noticing of early warnings and the consequent prevention of hostile events (Beitlich, 2014; Nussbaum, 2017). Numerous are the organisational and technological solutions that have been introduced with such a purpose. By way of illustration, major public and private entities have instituted Security Operations Centres (SOCs) (www.ibm.com; Ahlm, 2021; ISF, 2019) or similar structures having, among other functions, that of averting cyber incidents by conducting, *inter alia*, activities of Event Management, Continuous Monitoring and of Vulnerability Assessment and Penetration Testing (VA/PT). Cybersecurity departments have traditionally been using firewalls to monitor inbound and outbound network traffic and bar that suspected to be malicious (www.cisco.com; www.fortinet.com; www.kaspersky.com). These computer network security systems have, more recently, been complemented by such technological solutions as Intrusion Detection (IDS) (www.fortinet.com; www.checkpoint.com) and Prevention Systems (IPS) (www.fortinet.com; www.paloaltonetworks.com; www.gartner.com), Endpoint Detection and Response (EDR) (www.fortinet.com; www.gartner.com; Aarness, 2023), as well as Security Information and Event Management (SIEM) (www.ibm.com; www.microsoft.com). The adoption of such and other technological instruments is surely essential. Notwithstanding their specific functions, they aim at and contribute to not only detecting but also preventing hacking attempts, thanks to the fact that they shield networks and systems in an automated manner from suspected activities and allow to collect technical data that may prove fundamental for investigating previous malicious cyber events and predict future ones. Nevertheless, they remain reactive tools in the sense that they assume the spotting of an Indicator of Compromise (IoC). In other words, they

operate, primarily with mitigation purposes, only after an endpoint or network has probably already been breached (CrowdStrike, 2020; www.fortinet.com).

In order to compensate for technology's shortcomings and possible fallibility, in recent years, some experts have been recurring to behavioural and predictive analytics. Numerous have been arguing how gathering non-technical data is key for forecasting the occurrence and timing of cyber incidents. As per Anup Sharma et al., a direct correlation exists between social, political, economic and cultural events occurring in the physical world and COs. They thus postulate that comprehending such relationship may assist in the elaboration of preventive measures against digital breaches and elaborate a threat-based attack model with such a purpose (Sharma *et al.*, 2013). David Maimon et al. similarly focus their analysis on cyber-dependent crimes and propose an extended version of the SKRAM model advanced by Donn B. Parker (Parker, 1998). More specifically, they contend that examining the five elements of the framework (i.e., individuals and groups' *skills*, *knowledge*, *resources*, *access* to the facilities or information systems intended to be targeted and *motivation* to engage in online criminal activities) is not sufficient for anticipating cyber threats. The authors introduce, therefore, two additional conditions. First, organisations must additionally seek to comprehend possible attackers' personality traits and demographics, as well as circumstances that may affect their decisions to launch cyberattacks. Secondly, they must more generally forge their cyber prediction strategies also considering classical criminological theories (Maimon *et al.*, 2017). Adam Dalton et al. finally claim that cognitive augmentation, and in particular information foraging, permits to overcome some of the issues arising from the generation of big data (www.oracle.com) by balancing human intuition with automation and, therefore, to unearth public available but unconventional resources that may be employed as training datasets for developing algorithms seeking to forecast cyberattacks (Dalton *et al.*, 2017).

Notwithstanding the value of both technical and non-technical data, it is here important to note that both typologies, as well as the technological tools that may have been used to gather them and/or to prevent intrusion attempts are of no utility if they are not integrated within defined and structured processes. Cyber warning intelligence models have been elaborated with the precise objective of providing a high-level operating scheme within which processes, technological solutions, as well as roles and responsibilities are to be delineated and rendered interoperable. As above, the analysis of cyber warning intelligence models is here limited to present the most renowned and utilised ones. In particular, surely worth mentioning is the Lockheed Martin Corporation's Intelligence-Driven Defence model, constructed by Eric M. Hutchins et al. The model has specifically been designed for the prevention of cyber intrusions by Advanced Persistent Threat (APT) groups. The latter are well-organised and highly likely state-backed actors that generally aim at exfiltrating data, undermining or impeding the delivery of a service and/or at acquiring the capability to do so in a succeeding point in time and that have the know-how, as well as the substantial economic capital and resources that allow them to exploit different attack vectors in often strategic information technology (IT) infrastructures and, once they have been penetrated, to maintain the level of discretion useful to deceive and bypass their security systems and remain unobserved for an extensive timespan (NIST, 2021; www.apt.securelist.com). In order to address such sophisticated threats, Hutchins et al. contend that it is essential for organisations to adopt network defence techniques permitting to acquire information superiority over adversaries, track the latter's behaviour and progressively decreasing the likelihood of success of their intrusion attempts by pre-emptively enhancing cybersecurity solutions. The Lockheed Martin Corporation's model rotates, in fact, around the identification, collection, correlation and analysis of indicators of suspected activity throughout the so-called Cyber Kill Chain (Hutchins *et al.*, 2011). The notion of the Cyber Kill Chain has been coined by the Corporation but is a renowned phased process

describing – according to the perspective of attackers – the evolution of computer network penetrations (i.e., reconnaissance, weaponisation, delivery, exploitation, installation, command and control, actions on objectives). More specifically, Hutchins et al. note that upstream cyber intrusions is an activity of information-gathering from the part of threat actors aimed at selecting their target(s), scanning their environment and at identifying potentially exploitable vectors for attack. Following such a preliminary stage, attackers develop a weaponised deliverable (e.g., Adobe Portable Document Format (PDF) or Microsoft Office documents) and successively transmit it to the targeted network (e.g., through email attachments, compromised websites, etc.). After having acquired access to the victim system, a remote access trojan or backdoor is installed to allow persistence *in situ*, a Command and Control (C2) channel is established and intruders can finally proceed with acting to attain the intended objective of the attack (e.g., exfiltrate or spoil data, sabotage or degrade systems, financial gain, etc.) (www.lockheedmartin.com; Sakuraba *et al.*, 2008; Bou-Harb *et al.*, 2014; Mandiant, 2023). The merit of such a framework – and the reason of its success – does not, however, merely reside in the support that it offers in the analysis of malicious COs. On the contrary, it also permits defenders to enhance their visibility into their digital infrastructure (i.e., to verify the possible presence of vulnerabilities and hostile actors exploiting them) and to leverage the actionable intelligence acquired to formulate investment programmes, implement corrective actions and measure their effectiveness (Hutchins *et al.*, 2011).

Given its practical value, the Cyber Kill Chain is integral part also of the framework published by Michael Robinson et al. The latter consists in an adaptation of the original Lockwood Analytical Method for Prediction (LAMP). The influence of the LAMP is apparent in the articulation of the paradigm into the twelve stages that have been illustrated above. Following a first and second phase during which organisations' cybersecurity departments are recommended to identify the specific issue (i.e., to acquire the most accurate comprehension

of the scope, method and objective of the attack possible) and the actors engaged, Robinson et al. suggest, in fact, the use of the kill chain as an analytical instrument through which to gather and systematise intelligence information concerning adversarial actors' manoeuvres. The authors admit that identifying signals of suspicious behaviour before the delivery of weaponised payloads by APT groups is particularly complex owing to the vastity of the spectrum of sources and environments to scrutinise. Nevertheless, they encourage defenders to concentrate their efforts in enhancing such capability since it may serve to effectively counter an adverse cyber event before its occurrence. Contributing to serving such ultimate objective, the fourth phase of the framework is represented by the determination of possible future scenarios of attack. Robinson et al. note that hackers are inclined towards certain computer methods according to their preferences, expertise and available resources. Being able to associate tactics, techniques and procedures (TTPs), as well as the underlying technological capabilities and limitations, with the respective player(s) recurring to them is key to forecast the latter's intent, motivation and courses of action. The level of difficulty in conducting such prediction and detection analyses may progressively increase in relation to the actors involved and to their organisational and technical sophistication. Nonetheless, the authors stress the importance of constantly collecting, examining and monitoring even undetermined signals and patterns, awaiting that they may successively be employed to draw correlations and inferences. The process delineated by the model further progresses with the determination not only of any possible scheme that intruders might follow, but also of their respective fundamental steps. Robinson et al. explain that "[w]ith no real boundaries established on the Internet, guarding cyber borders from attacks requires conceived multi-layers of defence to implement detection systems that are honed to identify clusters of activities *by recognising* patterns of behaviour *suggesting that* a targeted objective (or mission) is underway". As they further point out, "[o]ne-off activities may not be a strong indicator of a future cyberattack and the activities

might go unnoticed *but* [w]hen activities, attack points and methods are clustered together, a pattern can be identified and analysed resulting in predictive behaviour". As a result, "defence systems must be able to identify an active kill chain 'focal event' in its early stages to *interrupt* the event flows to thwart an attack from progressing and identify the attacker or their technique footprint to defend against subsequent occurrences" (emphasis added) (Robinson *et al.*, 2012). Succeeding steps of the framework are the creation, collection and monitoring of indicators of events that, being required for developing a certain scenario, may, if detected, testify not only to the occurrence of a breach and its state of evolution, but also to the *modus operandi* selected by the threat actor(s). In this regard, the model comprises four phases dedicated to the thorough study of the attack scenario in question. Competent authorities and officers are exhorted to verify the consistency between the scenario originally portrayed and that highlighted by indicators, employ the former as a benchmark for forecasting future developments while properly reassessing it in the case that additional information is collected and some of its elements appear unviable, as well as to confirm the resistance of indicators to deception attempts from adversaries or other distortions that may impact the analysis. The process finally concludes with the examination and contingent execution of strategic and tactical options (Robinson *et al.*, 2012).

Third intelligence-driven cyber defence framework described here is the one proposed by the Intelligence and National Security Alliance (INSA). The model pursues an approach similar to that of Robinson et al.'s revision of the LAMP. It consolidates, in fact, structural elements of traditional I&W methodologies with cyber threat models to formulate a paradigm that could serve as a high-level guideline for public and private entities in their efforts to precede and thwart malicious cyber scenarios. The number of steps in which it consists is, nonetheless, halved into the following seven: the identification and prioritisation of assets, the prioritisation of threats, the assessment of possible hostile courses of action, the decomposition of anticipated scenarios into

indicators, the devising and testing of counter-measures, the alignment to the intelligence cycle and the implementation of proactive solutions. Researchers have founded the model upon the assumption and empirical observation according to which no organisation can construct a perimeter of security encompassing the totality of its assets (e.g., data, personnel, devices, systems, facilities, etc.), hence the necessity to discern them on the basis of their criticality for the organisation's interests and objectives and to accordingly determine their level of protection. In a similar manner, the magnitude of the current cyber threat landscape is such as to impede the identification and eradication of any possible menace. In other words, hunting threats in cyberspace is particularly demanding even for government bodies and large corporations that, notwithstanding their superior cyber maturity, are exposed to a vaster range of threats due to their strategic importance. Moreover, increased is the risk that, despite the considerable resources allocated, such efforts result ineffective in preventing adversarial cyber events due to their inefficiencies. The report elaborated by the INSA thus recommends to determine the ten or dozen of threats that may have the most serious impact on key assets identified and to focus on mitigating them. According to the model, such activities of asset and threat prioritisation are preliminary to the succeeding development of possible courses of action that malicious actors may follow to the detriment of organisations. In this respect, additionally to the Cyber Kill Chain, the INSA suggests the use of the MITRE Corporation's Adversary Tactics, Techniques and Common Knowledge (ATT&CK) methodology and that of Structured Analytic Techniques (SATs) (INSA, 2018). The former is an online freely accessible knowledge base of tactics and techniques that state and non-state entities have been observed following in cyberspace and that, having been curated with the objective of enhancing defenders' capabilities of malicious behaviour detection, has been serving as a practical conceptual tool to gather threat intelligence, verify and ultimately strengthen the solidity of cyber intrusions defences by simulating attack scenarios (www.attack.mitre.org). The latter are, on the

contrary, techniques traditionally formulated within the intelligence circles but increasingly employed by the private sector as well to assist in the elaboration of solid analyses and estimations despite a congested, incomplete and ambiguous information environment, as well as human biases and limitations (Heuer and Pherson, 2011; US Government, 2009). Following the development and assessment of adversary courses of action, the INSA framework proceeds with their decomposition into indicators, namely analytical judgements founded upon evidence gathered that serve to identify patterns, developments or actions that malicious actors may undertake. Researchers have not established a pre-determined number or range of indicators to be delineated for each assessed course of action. In contrast, their number is contingent upon the circumstantial considerations of analysts who might, in fact, need a variable number of indicators for distinguishing that various scenarios are emerging. Contrarily to Hutchins et al. and Robinson et al., researchers at the INSA additionally recommend the use of the Indicators Validator Model in order to exclude indicators that may be common to multiple scenarios and focus on those that may be beneficial to adequately recognise a specific course of action. Nevertheless, they concur in affirming that the spotting of indicators is not synonymous with an occurred intrusion into a given IT infrastructure but that it may testify to the manifestation of an anticipated sequence of events. As it is further pointed out, they allow to comprehend the nature and timing of appropriate corrective actions. More specifically, competent authorities and officers are exhorted to set counter-measures for each indicator and regularly test them so as to ensure their rapid and effective implementation once a series of indicators alerts to the emergence of a certain adversary course of action. Similarly to the initial stages of the process, a prioritisation effort is requested here as well since organisations inevitably cannot forecast any possible scenario, let alone allocate and maintain the operability of the resources necessary to handle those that, notwithstanding their potentially nefarious effects, are improbable. In other terms, defenders must concentrate on those that

are assessed as having increased levels of probability and perilousness for organisations' key assets. Finally, as per researchers at the INSA, once information relating to the indicators previously enumerated is collected and recorded to identify intelligence lacunae, direct and prioritise the collection requirements to address them, the recommended cyber I&W programme is in place and organisations can proceed with the execution of counter-measures (INSA, 2018).

The studies described above have further been pursued and advanced by Bilyana Lilly et al. Similarly citing the Cyber Kill Chain concept, the authors reiterate and synthetise, in fact, the key observation according to which "[t]he current strategies that defenders employ are based predominantly on detecting cyber incidents at the early or later stages of a cyberattack cycle but seldom prior to the delivery of a weaponised payload to the defenders' networks" (Lilly *et al.*, 2021). In light of the elusiveness of prediction and – to a lesser extent – resilience in states' cybersecurity strategies and practices, the authors propose the RAND Corporation's Scalable Warning and Resilience Model (SWARM). The model maintains the objective of enhancing the abilities of cyber defenders to predict and anticipate malicious penetrations into their systems before their occurrence but more explicitly states the consequent one of augmenting the latter's resilience vis-à-vis cyber threats. In order to attain such dual objective, the framework is articulated into four phases. The first phase consists in the identification and prioritisation of possible cyber adversaries (Lilly *et al.*, 2021). A previous version of the model published by the authors had consolidated the first and second stages of the Robinson et al.'s approach and had revolved the outset of the proposed cyber warning intelligence process around the definition of Priority Intelligence Requirements (PIRs), namely a series of primary questions guiding intelligence collectors and analysts to determine the information needed to inform their judgments over a given issue. Four were the key areas to which PIRs were related. In particular, dedicated groups of experts were firstly entrusted with the determination of threat classes posing the major

risk to their organisation's information systems. Secondly and thirdly, they were recommended to investigate the typology of threats behind prior incidents both involving the specific organisation and others in its sector and to evaluate additional but still unknown threat sources. Finally, they were called to outline a *modus operandi* for each malevolent actor identified, comprehend their motives and objectives, detect anomalies in their expected behaviour, explore possible exploitable vulnerabilities and attack vectors, as well as to determine adequate measures to mitigate the effects of successful cyberattacks (Lilly *et al.*, 2019). Such scheme has been reproduced in the SWARM. The latter better emphasises, however, how the categorisation of the concerned organisation within a certain sector and the study of the relative cyber threat environment evolution are prerequisite for identifying actors that might attempt to penetrate defenders' information systems. Organisations active in a certain sector are likely confronted by classes of cyber threats that differ from those of other sectors. The rationale behind the SWARM's initial steps is thus not to elaborate an exhaustive catalogue of cyber malevolent actors but to identify and classify – according to a combination of various logics (e.g., motivation, capabilities, etc.) those that, with solider confidence, are expected to target the precise organisation implementing the model. The second phase is contrarily focused on leveraging the information derived from the PIRs previously identified to lead further intelligence collection efforts. Lilly et al. emphasises the importance of adopting a tailored "all-source approach encompass[ing] not only technical but also non-technical or geopolitical indicators [that] can improve the early detection and warning of cyber incidents by allowing defenders to scan holistically the entire operational space for potential behavioural and environmental triggers that can signal an adversary's intent to initiate a cyber incident" (Lilly *et al.*, 2021). In sum, the authors urge information security professionals to gather, analyse and operationalise Cyber Threat Intelligence (CTI) from a vast array of open and closed sources. They concur with the assumption behind the above-mentioned studies by Sharma, Maimon and

Dalton et al. according to which non-technical data can support the prediction of hostile behaviour in cyberspace. Nonetheless, besides arguing for their correlation with technical information, they suggest the adoption of the Analysis of Competing Hypotheses (ACH) methodology as an analytical tool that, thanks to its practicality, allows even organisations having limited resources to understand the attackers' motivation(s) and, on the basis of observations of geopolitical events and/or other sets of circumstances in both the physical and digital environments that may serve as incentive for engaging in adversarial activities, to predict and halt possible future attack scenarios. The third phase better details such process. Following the construction of an as comprehensive knowledge base about adversarial actors and the threats posed by them as possible, the given organisation is recommended to decompose the expected malicious behaviour into the TTPs in which it might materialise along the Lockheed Martin's Cyber Kill Chain. With this regard, similarly to but also elaborating on the INSA framework, Lilly et al. suggest the adoption of the MITRE PRE-ATT&CK and ATT&CK taxonomies. The latter are set as preferred threat modelling frameworks in view of their usability, already widespread diffusion and effectiveness. Nonetheless, the authors leave flexible defenders' choice to recur to other tools that may be judged as more germane to their needs. The fourth and final phase is dedicated to the operationalisation of the threat modelling through the performance of activities of threat emulation. In such concluding stage of the paradigm, more apparent becomes the objective of enhancing resilience in cyberspace. Organisations are called, in fact, to appoint a Red and Purple Team (CrowdStrike, 2023) in charge with the conduction of penetration tests to identify and assess potential vulnerabilities and/or relevant lacunae in the visibility within the organisation's information infrastructure in order to strengthen its defensive systems (Lilly *et al.*, 2021).

Chapter Three

Synthetising a Framework for Cyber Early Warning

The examination of the primary cyber indications and warning (I&W) intelligence models presented in the previous chapter has allowed to track the practices leveraging indications intelligence and structured analytic techniques that experts judge as crucial to construct proactive cybersecurity strategies, as well as to bring to light their respective strengths and weaknesses. As an illustration, Hutchins et al. have adopted an innovative attack-centred approach focused on gathering intelligence, promptly identifying indicators of suspicious cyber activities along a kill chain and implementing the appropriate corrective measures. Yet, such approach maintains some significant post-hoc elements. The proactive and continuous monitoring of a certain organisation's information technology (IT) infrastructure is crucial to comprehend not only its vulnerabilities but also the intent and capabilities of malicious actors targeting it. Nevertheless, the outcomes of the analysis of the information gathered through such activities would be partial as they are founded upon the mere examination of previous incidents on that particular infrastructure and hence do not consider data relative to intrusions that have not been detected and/or that have not yet compromised the organisation but may do so in the future. In contrast, the organisation must conduct intelligence-gathering both within and outside its perimeter to identify and prioritise the major threats generally associated with its respective sector. Such efforts, albeit neglected by the authors, are vital to adopt thoughtful solutions that are not merely able to counter the series of circumstantial threats observed but also promise to be effective for

novel attack scenarios. The criticality of developing scenarios serving as analytical instruments to predict cyber incidents has correctly been stressed by the model published by Robinson et al. The framework's twelve phases recalled from the original Lockwood Analytical Method for Prediction (LAMP) are probably excessive in number and risk rendering it complex in implementation. Yet, the author of the present work majorly criticises their ultimate objective of adopting a so-called "aggressive offensive counter-cyberattack posture". Robinson et al. have stated their intent of promoting practices pursuing logics antithetical to those of common yet static and reactionary cybersecurity measures. The approach suggested to do so is, however, judged as not only inadequate to augment defenders' resilience towards digital threats but also as potentially escalatory. Finally, the Intelligence and National Security Alliance (INSA) framework, in accordance with the constantly increasing density of today's threat landscape but contrarily to the previous two models' focus on Advanced Persistent Threat (APT) groups, has the merit of having expanded the pool of cyber threats to which it may be applicable. Nonetheless, the model describes the execution of proactive counter-measures as final step of the proposed cyber I&W process and subordinates it to the completion of each of the previous phases. Such rigid linearity that characterises the model does not reflect the concrete exigencies of the personnel responsible for handling alerts of cyber events or actual incidents and may seriously affect cyber warning intelligence efforts. Defenders might be in the urgency of adopting a certain precautionary measure to impede a mere alert from transforming into a proper cyber compromise and awaiting the conclusion of the entire programme might cause considerable delays and harms.

The author of the present research project concurs with some experts in stating the criticality for defenders of enhancing their capabilities to detect potential intrusions in the earliest stage of the Lockheed Martin Corporation's Cyber Kill Chain possible. The ability to spot digital breaches into one's networks and systems in advance of substantial harms and more rapidly halt

them would represent a considerable advancement of most organisations' current cybersecurity status. Cyber detection is of paramount importance (Kott, 2014). However, it must intervene only in case of failure of cyber prediction efforts. As immediate as it might be, it remains, in fact, the reaction to an intrusion that could have been forecasted and prevented (Ramaki and Atani, 2016). As affirmed by Kris Oosthoek and Christian Doerr, "[t]he unrecognised presence of malicious actors within the trusted enterprise network boundary effectively signifies an intelligence gap in computer network defence" (Oosthoek and Doerr, 2021). Organisations can no longer afford to pursue cybersecurity strategies relying on the mere detection of – let alone response to – malicious cyber behaviours. On the contrary, they must aspire and act to pre-empt them. In the present section the author proposes, therefore, a high-level cyber I&W paradigm that attempts to synthetise the strengths and address some of the weaknesses noted above in extant models. The decision not to forge a novel methodology resides on the author's acknowledgement of the value and utility of previous research but also of the need to limit its shortcomings and pool its findings into a single model in order also not to overwhelm organisations with procedures that risk falling by the wayside. Denounced here is the absence of a structured – common or sectorial – model or approach, adopted at a national or international level, that, on the one hand, recognises the heterogeneity and complexity of both organisations and the cyber threats to which they are exposed and that has, on the other hand, proven effectiveness in the forecasting and preventative handling of cyberattacks (Papastergiou *et al.*, 2020). As per the author of the present work, the SWAMP framework by Lilly et al. constitutes the most valid and comprehensive attempt to remediate such a lacuna. Nevertheless, unverified are not only its knowledge and sequel among organisations but also its applicability and potential for concrete positive effects. Organisations, especially those in the public sector, tend to have an aversion to structural changes or, at least, to implement them according to extended timings that do not conciliate with the dynamic evolution of the cyber landscape. The

cyber early-warning framework proposed here thus seeks to consolidate the actions and processes that, being essential for the efforts in the prediction and prevention of adverse COs, organisations are recommended to enforce and integrate within their cybersecurity architectures. The model is primarily intended for public bodies and large- and medium-sized private corporations that hence already have relatively satisfactory levels of cyber maturity and more resources to invest in cybersecurity. Nevertheless, the model contains several best practices that may serve as guidelines for the design and implementation of cyber defences of small companies as well. The model voluntarily maintains a degree of generality that ensures its customisation and applicability to various environments. The typology of cybersecurity measures needed is, in fact, function, *inter alia*, to the dimensions, architecture and strategic value of the organisation in question, the sector in which it is active and the relative threat environment, as well as to its cybersecurity posture and mechanisms already available.

The proposed paradigm is informed by the principles of comprehensiveness, actionability, efficiency and timeliness. The model encompasses, in fact, the entire spectrum of the phases that precede cyber incidents and suggests operational best practices that contribute to predicting and averting them. It is additionally not focused on a single typology of threats to which solely organisations operating in certain sectors are exposed. On the contrary, it is devised as a high-level framework with the versatility necessary for its modulation to public and private entities that differ in structure and cyber threat landscape. Moreover, it recommends a series of measures that are relatively straightforward to implement since they may often integrate – with the purpose of ameliorating – procedures and processes that have already been established. Dual is the consequent advantage. On the one hand, by so doing, defenders are able to minimise efforts and maximise resources already available. Proactively defending one's IT infrastructure by anticipating threats and threat actors' moves and implementing the appropriate counter-actions may be costly

as it demands extensive intelligence gathering and analysis endeavours and updated technologies that yet do not guarantee the successful prediction and prevention of cyberattacks. Regardless of their dimensions, organisations constantly have inadequate financial, human and technical capitals, hence the criticality of efficiently employing them. On the other hand, leveraging and boosting available capabilities favours a prompter intervention. Warning must, in fact, be issued as timely as possible in order to permit authorities to take calculated decisions and officers to consequently adopt the agreed pre-emptive measures (Grabo, 2015).

Contrarily to extant cyber warning intelligence frameworks, the one proposed here is, moreover, not phase-based. The articulation into phases surely guarantees order and systematisation. As mentioned above, it yet risks encumbering the implementation of models with a rigidity that induces the latter's uncritical application, contrarily discourages its more appropriate customisation to a given organisation and generates consequential delays. The present paradigm opts, therefore, to illustrate a series of actions that – organised on the basis of their common objective into five macro-areas – need to be considered not in their singularity but as a continuous and not necessarily linear process. More precisely, the first category encompasses actions that seek to estimate organisations' status quo. Preliminary necessary – yet not sufficient – condition that organisations must fulfil in order to predict cyber incidents against their IT infrastructure is, in fact, the acquisition of an in-depth understanding of their profile at a more systemic level. Accurate must be their understanding of the sector(s) in which they operate and the implications that this might have in terms of exposure to cyber risk. The belonging to a certain sector is not a deterministic indicator of the threat environment to which organisations are exposed. Yet, it might significantly simplify the determination of the nature of both the intruders and the intrusions that are more probable to target their systems. In other words, it is essential to understand what are the peculiarities, functions, key processes and related capabilities, as well as the

strategic value of one's sector(s) and to examine such factors also in consideration of the varying national and international political, economic and social dynamics that might affect them. This permits to identify the typologies of more common threats generally associated with those sectors, the malicious actors notorious for targeting them and the interests that the latter might have in compromising the networks and systems on which they rely (Lilly *et al.*, 2021). With the intent of facilitating organisations in establishing the definition and conceptual categorisation of their sector of belonging, Lilli et al. have recalled the sixteen critical infrastructure sectors identified in the Presidential Policy Directive/PPD-21 published by White House in 2013 (i.e., chemical; commercial facilities; communications; critical manufacturing; dams; defence industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials and waste; transportation systems; water and wastewater systems) (White House, 2013) and have complemented them with four additional categories (i.e., educational institutions; think tanks and non-governmental organisations (NGOs); dissident groups; inter-governmental and international organisations) (Lilly *et al.*, 2021). Such taxonomy is welcomed by the present research work as it is judged as a practical tool that not only conforms to the American doctrine but also expands on it allowing its application also to other contexts. Yet, it is to specify here that the lines between its categories might be blurred. In light of the profound interconnectedness that characterises today's national and international systems, organisations may belong to and surely depend on more than a single sector, hence the need to have a more comprehensive sight of the primary sectors relevant to the given organisation while prioritising the one(s) of belonging.

Further to a problematic tendency to overlook the profiling efforts described above, organisations additionally generally have an inadequate visibility of their cybersecurity status. Experts have repeatedly emphasised the gravity of such issue. Having a limited vista on one's cybersecurity perimeter

and maturity signifies, in fact, being unable to recognise and manage risks and consequently being more prone to fall victim to hostile cyber activities (Galinec and Steingartner, 2017). Diffuse among both public and private organisations is the tendency to overestimate their ability to defend their digital assets also owing to an often undue confidence on the technological solutions that they have implemented but to a scarce understanding of their functioning. Numerous of extant cybersecurity frameworks developed both in official documentations and within academic circles present as initiatory corrective recommendation that of setting up and constantly updating an inventory of devices, software, computer applications, systems and services encompassed within the organisation's perimeter in order to identify the critical information, data and systems and prioritise their protection (NIST, 2018; CIS Sapienza and CINI, 2017). Once key assets have been identified, organisations must understand what are their current abilities to protect them. In this respect, organisations must acknowledge that their cyber defence is not, however, merely guaranteed by technological solutions. Cybersecurity is not, in fact, a mere technical issue. On the contrary, a solid cybersecurity architecture is constructed upon formal and institutionalised processes, advanced technologies, as well as defined roles and responsibilities. Organisations must, therefore, act in parallel along all three dimensions and assess their respective status. More precisely, they must be aware of what are the processes in place, the subjacent technological tools in use and the organisational units responsible for their governance and execution. They must evaluate the strengths and weaknesses of each dimension, by considering, *inter alia*, the effectiveness and efficiency of the design and implementation of processes, the degree of integration among technologies, as well as the adequacy of the number and competences of the personnel allocated within the various departments. Recommended is also the conduction of Vulnerability Scanning (www.checkpoint; www.owasp.org) and Assessment (www.fortinet.com; www.imperva.com), Penetration Testing and Purple Teaming activities (Orchilles, 2022). In this initial stage, the latter two may not

benefit from the intelligence on threat classes and actors posing the most serious risk to the information systems of a given organisation and may not, consequently, be tailored to them in order to simulate more probable scenarios of attack. Yet, all four activities are fundamental to preliminarily assess the organisation's ability to prevent cyber incidents and, as a result, direct their efforts accordingly.

Once organisations have acquired a more comprehensive understanding of their profile and current cybersecurity posture, they must proceed with gathering data that may support in the identification and forecasting of major threats and possible attacks to their critical assets. As mentioned above, major organisations generally utilise Security Information and Event Management (SIEM) platforms collecting, correlating and analysing event log data from an ample range of sources across their IT infrastructure (e.g., users, endpoints, applications, cloud and networks) and alerting to possible anomalous behaviours in it (www.ibm.com; www.microsoft.com). Integrated with such platforms is often a ticketing system that allows to request Security Operations Centre (SOC) analysts or other IT department experts to manage a certain alert, namely to analyse a given Indicator of Compromise (IoC), perform – in case of incident – the actions delineated by the Incident Response Playbook (IRP) corresponding to the specific typology of cyberattack with the objective of containing, eradicating and recovering from it (Hollenberger, 2023) or to invalidate the ticket in case the alert revealed itself as a false positive (www.servicenow.com; www.ibm.com; Trost, 2023). Processes of Event and Incident Management may, moreover, be automated through the adoption of Security Orchestration, Automation and Response (SOAR) technologies that assist in the handling of alerts, thus reducing mean times to detect (MTTD) and to respond (MTTR) to incidents as well as limiting errors and operational inefficiencies (www.paloalto.com; www.microsoft.com). The integration of SIEM, IT ticketing and SOAR security solutions is, therefore, of paramount importance. They essentially are tools of cyber defence intended to support

analysts to detect and mitigate intrusion attempts or attacks. Yet, they additionally have an albeit indirect predictive function as they track and store valuable data concerning past cybersecurity events and incidents against organisations' infrastructures within a centralised console and thus serve as a repository of historical data allowing the identification of patterns of behaviour and, consequently, the forecasting of similar future attacks. Nevertheless, in order to acquire and develop one's predictive capabilities in cyberspace, collecting and analysing data merely from internal systems to spot threat indicators is insufficient. Those data are critical to further enhance visibility within one's cybersecurity perimeter, detect possible vulnerabilities and identify attack vectors that malicious actors more commonly attempt to exploit to penetrate it. However, they must be integrated with cyber intelligence (CYBINT) about possible emerging threats and zero-day vulnerabilities acquired through more proactive collection activities across external sources as well (Panagiotou *et al.*, 2021). As per a study conducted by the Intelligence and National Security Alliance (INSA), "effective cyber intelligence will begin to enable predictive, strategic warning regarding cyber threat activities, mitigate risks associated with the threat, enhance [the] ability to assess the effects of cyber intrusion and streamline cybersecurity into a more efficient and cost-effective process based on well-informed decisions" (INSA, 2021). Over the last decade, representatives of international institutions and agencies, domestic state entities, private corporations and scholars have been calling for adopting intelligence-led approaches to tackle cyber menaces (Roberts, Maxwell and Brown, 2017; Bonfanti, 2018; Pace, 2018; JD Work, 2022). Nevertheless, the concept of CYBINT remains unclear. In the present work, it is intended as the information resulted from the processing and analysis of data gathered both *within* or *through* cyberspace (*stricto sensu* definition) and following the conduction of all-source intelligence activities (*lato sensu* definition) with the purpose of reducing uncertainty over a certain cyber-related issue and support the decision-making process (Bonfanti, 2018). Moreover, organisations are here

recommended to consider all three CYBINT's levels of actionability. Randy Borum et al. have noted, in fact, that much of the debate has focused on tactical CYBINT and has, on the contrary, neglected the strategic and operational levels (Borum *et al.*, 2014). As the authors have argued elsewhere, such emphasis on on-the-network operations is evidently problematic as political and military authorities or senior managers may not receive the intelligence needed for their organisations' risk management policies (Borum *et al.*, 2015). As maintained by Cynthia M. Grabo, "[w]arning is an exhaustive research effort" (Grabo, 2015). The information systems community within both the public and private sectors must engage in Cyber Threat Intelligence (CTI) (www.crowdstrike.com) collection activities along two parallel trajectories. The first is internal to a given organisation's IT perimeter and has a reactive approach since it is focused on gathering data about cyber incidents already occurred (internal network and endpoint data) (Ernst & Young, 2014). In contrast, the second is external to the perimeter and has a more proactive approach since it encourages the scrutiny of data retrieved, *inter alia*, from the dark web and hackers for a (Dhake *et al.*, 2023), the geopolitical context, Information Sharing and Analysis Centres (ISACs) and Organisations (ISAOs), social media (Hernández *et al.*, 2016; Shu *et al.*, 2018), law enforcement reports and along the supply chain (INSA, 2018; Yucel *et al.*, 2020).

Gathering all-source intelligence is, therefore, vital for the purposes of cyber warning. Yet, the exclusively manual conduction of such activity is unfeasible. Mauro Conti et al. contend that "[t]he ever-increasing number of cyberattacks requires […] cybersecurity and forensic specialists to detect, analyse and defend against the cyber threats in almost real-time". As the authors further explain, "[i]n practice, timely dealing with such a large number of attacks is not possible without deeply perusing the attack features and taking corresponding intelligent defensive actions […]". They observe, nonetheless, that "such an intelligence would not be possible without the aid of Artificial Intelligence, Machine Learning and advanced data mining techniques to collect,

analyse and interpret cyberattack evidences" (Conti *et al.*, 2018). Current cyber warning intelligence frameworks have been accused of myopia by some researchers due to their often exclusive focus on either computational and automated tools or user-driven analytical methodologies and their consequent unappreciation of the potential offered by the combination of socio-technical methods within a single model (INSA, 2018). Over the past two years, Richard Carley has been investigating how to more efficiently develop early warning systems for cyber intrusions leveraging ML techniques. No publications on the matter have, however, been released by the author yet (www.minerva.defense.gov). It is nevertheless to be emphasised here that a general consensus exists in stressing the value of AI technologies to forecast adversarial COs. They promise and have already demonstrated, in fact, to be able to at least diminish the often-alleged asymmetries between cyber offence and defence and possibly offer a considerable strategic advantage to defenders (Banham, 2018; Parisi, 2019; Das *et al.*, 2022; www.ibm.com). As it has been noted, "[a]lgorithms *bypass the conundrum of cyber attribution as they* can identify the source *of a cyber operation* and neutralise it without having to identify the actor behind it" (emphasis added) (Taddeo and Floridi, 2018). AI and ML-based instruments will not guarantee the prevention of all cyberattacks but might have a deterrence function as they might complicate the accomplishment of attackers' objectives or reduce the benefits obtained from their attacks and raise the cost of engaging in such activities – for instance, by developing new capabilities and methods that will oblige attackers to deploy more sophisticated tools or that will increase their risk of exposure to defenders' retaliatory measures (National Academies of Sciences, Engineering, and Medicine, 2019). Furthermore, AI technologies assist IT analysts in collecting potentially valuable information for forecasting cyber incidents. Jacopo Bellasio et al. observe that "[t]he proliferation of existing sensors across a growing number of devices, as well as the development and use of new sensors, for example in the context of Internet of Things (IoT) and autonomous devices and

systems, will expand data collection capabilities and contribute to the development and collection of new data types". As they further point out, "[t]his trend is expected to be compounded by advances in data storage technologies which should result in increased data storage capabilities and in a quasi-ubiquitous accessibility of data" (Bellasio *et al.*, 2020b). Such advancements are surely positive as they would permit analysts to automatically gather, correlate and examine data to which they would otherwise not have access and, therefore, to elaborate more robust assessments. Yet, the exponential growth of the volume, variety and velocity of data, as well as their often dubious veracity raise serious issues. Analysts would highly likely be overwhelmed by information overload in the absence of computational support (Dupont, 2003; Aradau and Blanke, 2015; Hare and Coghill, 2016; Lim, 2016; Van Puyvelde *et al.*, 2017; Allen and Chan, 2017; Eldridge *et al.*, 2018; Regens, 2019; Gartin, 2019; Vogel *et al.*, 2021; Ish *et al.*, 2021). On the other hand, it is to be specified, nonetheless, that AI is not a panacea. Organisations must be aware of how their cyber predictive AI-enabled technologies operate and guarantee the quality of the data utilised to train the algorithms behind their functioning. As it has correctly been pointed out, "[a]lgorithms that are predicated on biases within learning structures are self-reinforcing and will produce progressively less accurate analysis" (Brantly, 2018b).

The author of the present research project further recommends to store all data collected within a Threat Intelligence Platform (TIP) (www.paloaltonetworks.com) that, integrated with SIEM, ticketing system, SOAR and other technologies in use by organisations, will constitute a centralised Early Warning System (EWS) portal and allow both the sharing (Pöyhönen *et al.*, 2019; Rajamäki and Katos., 2020; Mavzer *et al.*, 2021) and the analysis of information, whilst eschewing interoperability issues often associated with the use of distinct platforms for the production of intelligence and its diffusion (Rantos *et al.*, 2020). As illustrated by the renowned and already-cited Intelligence Cycle model (Davydoff, 2018) – and yet elaborating

here on it, once gathered, data must be easily accessible to all relevant parties in order to be processed and analysed. In the latter's regard, correlating and examining often unstructured data concerning cyber threats and extracted from a myriad of sources in order to derive from them actionable intelligence is undoubtedly complex. Organisations tend to limit their efforts to the gathering and analysis of merely technical data and to overlook, on the contrary, non-technical ones. Yet, albeit vital, identifying potential vulnerabilities within an application through the receiving of an alert from automated technologies or the conduction of structured activities of Vulnerability Assessment and Penetration Testing is not sufficient for estimating how, when or by whom those flaws might be exploited (Williams *et al.*, 2002). Hostile activities in the fifth domain might be performed by a plethora of *actors* with a similar plethora of *motivations*, *objectives* and *capabilities* (Bonfanti, 2018). As a consequence, gathering data permitting to elaborate hypotheses and inferences related to all such factors is fundamental to predict malicious scenarios and promptly diffuse the relative warnings. More specifically, organisations must understand what are the hacking tools available in underground communities, what are the functions and features of such assets, who are the individuals and groups more actively engaged in disseminating them and having the capabilities to exploit them to launch cyberattacks, as well as what are the motivations and objectives behind their engagement in adversarial behaviours in the digital environment (Samtani *et al.*, 2017). The present work has already vastly described the question of the increased density of cyberspace in terms of players active in it. Worth briefly discussing here are, therefore, the other factors listed above. In particular, as already mentioned, conventional cybersecurity processes tend to focus on possible vulnerabilities in networks and systems and to neglect the motivations and intents of malevolent actors that may exploit them (Robinson *et al.*, 2012). The latter have been observed launching COs for acquiring strategic edges over geopolitical rivals and/or monetary profit or for ideological, retaliatory and recreational purposes. On the other hand, evaluating the intent of actors in

cyberspace is surely more complex. Herbert Lin explains how cyberattacks and cyber exploitations respectively have the differing objectives of modifying, disturbing or damaging targeted information or networks and that of covertly stealing data, but share similar technical features that render their dividing line blurred and difficult to discern by defenders (Lin, 2012). Focusing on inter-state relations and transposing the classical notion of "security dilemma" to the field of computational technologies, Ben Buchanan claims that "[t]o assure their own cybersecurity, states will sometimes intrude into the strategically-important networks of other states and will *thus* threaten – often unintentionally – the security of those other states, risking escalation and undermining stability" (emphasis added) (Buchanan, 2017). Similarly to Lin, the author specifies how the inherent opacity of the virtual domain hinders the certain categorisation of detected hacks as cyber nuisances, low-level operations sending signals of discontent, a preparatory measure for a major cyberattack or as a grave cyber event comparable to a conventional aggression. Even admitting that such distinction would be apparent, the possibility that, in moments of heated tensions, the access to a certain infrastructure or the intelligence acquired over a preceding cyber intrusion with mere defensive purposes will allow the mounting of a disabling or degrading cyber offence cannot be excluded. In order to facilitate their comprehension of adversarial actors' objectives, motivations and capabilities – similarly to what recommended by some of the extant cyber indications and warning (I&W) methodologies presented in the previous chapter – defenders are exhorted to recur to the MITRE Corporation's PRE-ATT&CK and ATT&CK knowledge bases since, as per many, they represent the most exhaustive enumerations of pre- and post-compromise malicious tactics, techniques and procedures (TTPs) currently available (Strom *et al.*, 2020; Cassetto, 2023). The rationale behind the choice of such threat modelling tools as preferential ones corresponds to that adduced by Lilly et al. for their Scalable Warning and Resilience Model (SWARM). Nevertheless, numerous others have been elaborated (e.g., the Center for Cyber Intelligence Analysis and Threat

Research's Diamond model (Caltagirone *et al.*, 2013)) and organisations may opt for those considered more appropriate for their specific context.

Following the efforts seeking to preliminarily evaluate one's cybersecurity maturity and those dedicated to gather, correlate and examine all-source intelligence about major threats to one's critical assets, third macro-area of activities in which the I&W model proposed here is articulated concerns the development of possible threat scenarios that a given organisation might have to handle. In this regard, the author recommends pursuing the practices that have been described in detail by Robinson et al.'s adaptation of the original Lockwood Analytical Method for Prediction (LAMP) (Robinson *et al.*, 2012). One question is, however, to be better specified here. More precisely, recalling again the words of Cynthia M. Grabo, it is essential to emphasise that "[w]arning is an assessment of probabilities". Grabo claims that "it is a rare instance in which impending hostilities will be so evident, or the intentions of the aggressor so unmistakable, that warning is a virtual certainty […] [and] [i]t is*, on the contrary, more* likely that there will be some degree of uncertainty concerning the plans or intentions of the enemy even when a great amount of information is available and the collection effort has functioned extremely well" (emphasis added). As the author further explains, "the choice of th[e] term 'indication' (i.e., a sign, […] a suggestion, a ground for inferring […]) to denote the nature of warning intelligence was a realistic recognition that warning itself is likely to be less than certain and to be based on information which is incomplete, of uncertain evaluation or difficult to interpret" (Grabo, 2015). In a similar manner, Lilly et al. note that "I&W entails a probabilistic analysis, in which an analyst attempts to provide an assessment which is as realistic and objective as possible, given data and time constraints" (Lilly *et al.*, 2021). Warning is, hence, rarely a matter of certainties. Analysts are contrarily called to evaluate the likelihoods of certain courses of action in given circumstances and accurately communicate their confidence in stating that a specific scenario might emerge. In order to facilitate such activities, analysts are exhorted to

continuously collect, process, analyse and monitor indicators from various – internal and external – sources. Moreover, the EWS platform recommended above must be configured to trace and display the highest level of detail of gathered data possible and especially their source, as well as the chain of modifications through which they undergo throughout their enrichment process. It has been claimed that commercial CTI – to which organisations may recur to operationalise their EWS and more generally to forecast cyberattacks – lacks a defined and transparent methodology (Oosthoek and Doerr, 2021). Analysts are surely not demanded to verify every piece of CTI but, in this way, would have the possibility to do so and would be allowed to assess the reliability of data that would subsequently synthesise more robust inferences and judgements (Hettema, 2021).

Once organisations have determined more probable scenarios of attack and their respective focal events, created, collected and monitored indicators testifying to the emergence of a certain course of action, readjusted initial hypotheses according to the information and evidence gathered and in consideration of potential deception strategies of malevolent actors, they may proceed with verifying the robustness of their cyber defences and their capabilities to resist the expected hostile scenario(s). In other words, organisations are urged to replicate the blue, red and/or purple teaming activities conducted at the outset of the I&W process proposed to assess their original cybersecurity maturity status but adapting them to the key threats to which – as per the previous intelligence gathering and analysis – the given organisation is primarily and more eminently exposed. Given the immediate reference to the adversary emulation phase of the SWARM in this regard, major attention should here be drawn to the fifth and final macro-area of activities that organisations should perform, namely the one related to the issuance of alerts. The latter's criticality for the process cannot be overstated. Grabo affirms, in fact, that "warning does not exist until it has been conveyed to the [decision-]maker". In other words, "[w]arning is a judgment for the [decision-]maker" (Grabo, 2015).

Errors, deficiencies and delays in the communication of alerts to relevant stakeholders responsible for determining the approach to be followed in the handling of a certain issue might endanger previous efforts and the successful prevention of an adverse scenario. Further to the timeliness requirement already emphasised above, warning alerts must be apparent to their addressees. For such purposes, organisations must address what David Mandel terms the "communication mode preference paradox" and the "illusion of shared understanding" by defining a common lexicon and guidelines. More specifically, Mendel observes discrepancies in senders and receivers of information's preferred forms for communicating probabilities (i.e., verbal or numerical) which are further exacerbated by the absence of an unambiguous interpretation of the terms used (e.g., likely, highly likely, probable, etc.). The author of the present work, therefore, concurs with the author in recommending the use of numeric probabilities. Presenting probabilities as a numeric range, albeit imprecise, ensures in fact clarity and facilitates a more effective comprehension of analysts assessments by decision-makers (Mandel, 2022).

Chapter Four

Case Study: Italy's Cyber Threat Ecosystem

As succinctly illustrated in Chapter Two of the present research project, over the past decade, academia has been devoting increasing attention to the predictability of cyber threats and a dynamic body of literature on the issue has thus been emerging. Scholars, public and private research centres and cybersecurity experts have developed both analytical and numerical (Onoh, 2018; Ibor *et al.*, 2020) models to assess the feasibility and effectiveness of cyber defence early-warning mechanisms. Despite the promising contribution to the understanding and thus the countering of cyber threats more generally that they provide, such frameworks have, nonetheless, rarely been tested. A thorough understanding and common approach of how such cyber warning intelligence models should be implemented and coordinated with extant capabilities and mechanisms is currently lacking (Lilly *et al.*, 2021). The above-mentioned nebulousness surrounding the notion of cyber indications and warning (I&W) is surely a primary hindrance to the enforcement of intelligence-based cybersecurity models. To this are added the lack of transparency over the methodologies that should inform their implementation process, the scarce collaboration and sharing of related best practices both among organisations that already have structured and that utilise such frameworks and between these and other organisations that do not have such capability, as well as the inadequacy of financial and human resources both in the public and private sectors (INSA, 2018). Notwithstanding such and other issues, the operationalisation phase is crucial. If not implemented, no matter how well-designed it might be, a model remains a mere sequence of actions documented on paper but having no utility for organisations.

As stated above, the cyber indications intelligence mechanism proposed in Chapter Three of the present work is intended as a general baseline framework for informing prediction and prevention policies of cyberattacks. Nevertheless, it has specifically been devised to be applied to the Italian and American case studies. In order to do so, the following two sections are respectively dedicated to a more specific discussion of the most recent trends and developments in the cyber threat ecosystems of Italy and the United States and to a brief overview of the measures adopted by Rome and Washington with the objective of averting cyberattacks. Conducting a comparative analysis of major cyber threats to Italian and American entities is complex owing (in part but not exclusively) to the numerous difficulties in acquiring solid statistics on cyberattacks against them. Likewise, assessing the current Italian and American predictive power in cyberspace and the progress of their efforts in this sense is complicated, *inter alia*, by the general absence of a systematic approach in the adoption of their various measures and initiatives. Nevertheless, some key considerations relating to the two points may be derived from available data.

Similarly to – albeit to a lesser extent – the United States, Italy's status as one of the most advanced economies in the international arena renders it an appealing target for the numerous actors engaged in cyberspace (Bucci, 2012). Nevertheless, the threat landscapes to which the two states are confronted differ for certain aspects and are constantly evolving. In its 2023 National Cybersecurity Strategy, President Joe Biden's Administration has reiterated how mere defacements and other cyber nuisances have increasingly been supplanted by more sophisticated espionage and cyber-enabled influence campaigns, intrusions into the systems of critical services, ransomware attacks and intellectual property thefts (White House, 2023). Over the past two decades, the US has been accusing the People's Republic of China (PRC), the Russian Federation, the Islamic Republic of Iran and the Democratic People's Republic of Korea (DPRK) of being behind such malicious COs that seek to undermine Washington's political, economic and social interests (ODNI, 2023; Smith,

2022). Yet, they do not constitute a monolithic threat synthesisable under the label of "authoritative governments". On the contrary, China, Russia, Iran and North Korea generally adopt specific attack strategies and *modus operandi* in cyberspace (Rugge, 2018) that must not be deterministically associated with the nation-state in question but that need to be acknowledged as they may serve as useful indicators to prevent certain cyberattack types. More precisely, Richard J. Harknett and Max Smeets argue that, if the definition of cyberwar as the utilisation of computational assets to inflict violence and cause physical damage is accepted, "China is […] the most 'peaceful' cyber power" (Harknett and Smeets, 2020). In contrast to such states as the US, Russia, Israel, Iran and North Korea, China has in fact reportedly never been responsible for information operations aimed at the degradation or destruction of their targeted networks (Harknett and Smeets, 2020). Yet, China is notoriously one of the most active states in the virtual environment (Hachigian, 2001). As it has been claimed, "[t]he People's Liberation Army (PLA) does have access to considerable resources, human capital and engineering skill [such that] it might in principle overcome operational barriers to weaponisation but its observed operational focus and experience are concentrated on intelligence operations" (Lindsay, 2015). Beijing's intelligence-gathering campaigns in the information technology (IT) infrastructures of other nation-states have in fact been denounced for years (www.cisa.gov) and some Western scholars often depict China as "one of the states […] that has employed cyber espionage more extensively than any other country" (Gilli and Gilli, 2019). The Russian government has similarly intensively recurred to the digital space to launch espionage and intellectual property theft campaigns (FSB, 2014; SCRF, 2016; Maurer and Hinck, 2018; Nye, 2019). In contrast with Beijing, the Kremlin has, however, adopted a less restrained behaviour. Clamorous have been the numerous influence operations in cyberspace, as well as the targeting of American and European critical infrastructure systems (ODNI, 2017; Jamieson, 2018; www.cisa.gov). Following the Russian invasion of Ukraine in February

2022, US cybersecurity authorities and their Five Eyes partners published a joint advisory alerting about increased risks of cyber offenses launched by threat actors differently affiliated with the Kremlin in retaliation for perceived cyberattacks against Russian targets or for the provision of any support to Kiev (Kaminska, 2022; Lewis and Wood, 2013). The report recalls, in fact, that Russia has proved to be able to compromise IT networks, maintain persistent access to and exfiltrate confidential information from them, as well as to deploy sophisticated malware to disrupt critical infrastructures (CISA, 2022). According to experts, such a prowess in cyberspace has, on the contrary, not yet been attained by Iran. Albeit constantly enhancing its cyber capabilities, Teheran has thus far generally altered malware already available in the criminal market but without inserting in them destructive features (Lewis, 2019). Iran tends to launch cyberattacks on poorly defended American targets to protest against Washington's presence in the region and retaliate against its sanctions and cyber covert actions (www.cisa.gov; Craig and Valeriano, 2016; Lewis, 2019). Finally, North Korean malevolent actions in the digital arena have generally been motivated by the will of generating revenue for pursuing Pyongyang's nuclear ambitions and other interests. North Korean state and state-sponsored agents are hence usually engaged in such criminal activities as the theft of crypto-currencies and ransomware operations (www.cisa.gov).

In contrast to Washington, Rome has traditionally been less vocal in publicly denouncing rival governments' hostile activities in cyberspace. In its National Cybersecurity Strategy 2022-2026, no explicit mention is made to either China, Russia, Iran or North Korea. In this regard, it is interesting to note that, according to the latest Report on Security Intelligence Policy relative to 2022, the activity of state or state-sponsored groups against Italian targets has slightly increased (3 percentage points) over the past year but merely represents 26 percent of the total number of hacks detected by the Italian intelligence services. Despite the complexities associated with attribution in cyberspace, the latter have been able to identify the perpetrators of the cyberattacks in more than

80 percent of the cases spotted. The above-mentioned report thus classifies the hacks based on the typology of the malicious actors responsible and, further to the minimal increase in cyber espionage campaigns against a decline in that by hacktivists, it reports a significant increment in the figures relative to cyber criminal activities (47 percent of the total, corresponding to an increase of 33 percentage points compared to 2021). Such a rise is, however, to be interpreted in light of the evolution from the tendency of spreading highly-sophisticated malware towards that of using more common cyber tools available in the deep and dark web that the analysis of the TTPs employed has emphasised. The rise is, thus, in part attributable to the fact that state and state-sponsored agents have been using instruments generally associated with cyber criminals, very likely with the intent of concealing their identity (Sistema di Informazione per la sicurezza della Repubblica, 2023; Martino, 2019). As explained above, over the past years, China, Russia, Iran and North Korea have been accused by the United States and its partners for hostile and irresponsible behaviour in cyberspace. Nevertheless, charges invoked by Washington are not limited to the direct engagement of their national authorities in cyber malicious activities against foreign entities. Beijing, Moscow, Teheran and Pyongyang are commonly held responsible also for turning a blind eye to and, on the conditions that they do not compromise national assets, even encouraging cyber criminals, as well as for recurring to them to maintain plausible deniability (Borghard and Lonergan, 2016).

Italian security services have additionally observed that the use of malevolent tactics in cyberspace to the detriment of public targets – 43 percent of the total – diminished by 26 percentage points between 2021 and 2022. Cyberattacks primarily concerned the central state administrations (62 percent of the total, a value incremented by 6 percentage points) and the IT infrastructures of local authorities and medical facilities (20 percent of the total). On the contrary, preferential targets of malicious cyber activity have been the networks and systems of Italian private entities. More precisely, they accounted

for 56 percent of the total cyber threat events detected throughout the year, corresponding to a growth of 32 percentage points in comparison to the outcomes of the analyses from the preceding year. Within such figure, particular relevance had the digital infrastructures or IT services, transportation and banking sectors. They represented respectively 22, 18 and 12 percent of the cyberattacks spotted against private organisations, signalling an increase of 16 and 5 percentage points compared to 2021 for the IT and banking sectors and the invariability of the data related to the transportation one (Sistema di Informazione per la Sicurezza della Repubblica, 2023). Italian official documentations consulted for the present research project report, nonetheless, contrasting data over the most common techniques used by threat actors to launch cyber operations against public and private entities. According to the already-mentioned 2022 Report on Security Intelligence Policy, the major techniques identified were malicious domain name registrations, malware (spyware, rootkit, keylogger, ransomware), SQL injection and blind SQLI, uncategorised, bug hunting (scanning, pad, backdoor, targeting) and the exploit of known vulnerabilities (Sistema di Informazione per la Sicurezza della Repubblica, 2023). On the contrary, the Italian National Cybersecurity Agency (ACN)'s recently-published Annual Report to Parliament has revealed that, in 2022, the Computer Security Incident Response Team (CSIRT) instituted at the Agency handled 126 cyber incidents and a total of 1094 cyber events (with an average of 10,5 cyber incidents and 90 cyber events per month and a pick of 118 cyber events in February 2022). Predominant techniques among these figures were the diffusion of malware via email, phishing, brand abuse, ransomware, vulnerability exploitation and information disclosure. The ACN has, nonetheless, laid particular emphasis on ransomware and Distributed Denial of Service (DDoS) attacks. The former have been observed majorly targeting private organisations (81 percent of cases detected) active in the manufacturing, technological and retail industries. The remainder 18 percent of targets of ransomware attacks belonged, on the contrary, to the public administration.

Such typology of cyber operations (COs) – followed by DDoS and malware – is, in fact, that more exploited to target Italian public institutions (ACN, 2023a).

Finally and similarly to the American case, it has been observed that the majority of the malicious COs (53 percent) identified by the Italian intelligence services in 2022 were aimed at acquiring an economic or strategic edge over their target. Significant were also the figures (31 percent) related to cyber events seeking to undermine the credibility or reputation of the target. Such an analysis interested in investigating the objectives of the various hostile cyber actions has delivered a converse picture in comparison with that of 2021. Over a year, the statistics of COs with the purpose of ensuring an economic or strategic benefit to the attacker and that of discrediting a certain organisation grew by 44 and 30 percentage points, respectively. On the contrary, albeit directed at the systems of key national ministries and major providers of electronic communications services and conducted via structured tactics and sophisticated instruments, cyber espionage campaigns – a constant against US entities – diminished by 20 percentage points and only had marginal numerical values. As a consequence, equally converse is the picture resulted from the categorisation of spotted malevolent cyber events based on their outcomes. More precisely, the increment of cyber criminal actions has manifested itself with the rise of identity and/or credential thefts (53,5 percent, i.e., a rise of roughly 48 percentage points) aimed at monetary profit or at conducting further hostile actions. Similarly and in accordance with the surged incidence of COs with defamation purposes, substantial was the number (approximately 31 percent of the total, increasing by 30 percentage points) of cases of cyber offences seeking to inhibit the supply of services by recurring to digital tools able to delete data and programmes within the systems of targeted machines, thus causing their inoperability. Finally, the sharp fall-off of detected cyber espionage campaigns has rendered inappreciable the number of data exfiltrations (Sistema di Informazione per la Sicurezza della Repubblica, 2023).

Chapter Five

Assessing Italy's Predictive Power in Cyberspace

In line with a recent general tendency, Italian cybersecurity experts within both governmental bodies and large- and medium-sized corporations have expressed dissatisfaction with current cyber defence mechanisms due to their evident inadequate capability to avert cyber malicious events (Wickes, 2021). The Italian National Cybersecurity Agency (ACN) has noted that four are the primary causes behind cyber incidents against national entities. Firstly, the latter have been observed adopting erroneous security and access credential management policies that are devoid of solid user authentication mechanisms to access services and that rarely put in place mitigation actions following data breaches. Secondly, organisations' cyber infrastructures tend to rely on obsolete versions of information technology (IT) and operational technology (OT) devices and systems that have been supplanted and that, having providers ceased to offer assistance and maintenance services for them, are more vulnerable to cyber intrusions. Similarly to the American context, the vast majority of today's malevolent cyber events against Italian targets are the outcome of the absence or inadequacy of measures of cyber hygiene, security and defence that thus leave their perimeter exposed to even already known and patched vulnerabilities. Thirdly, scarce is among organisations the compliance with sectorial best practices recommending a secure architectural design of networks, an active management and maintenance of systems, as well as the definition and implementation of schemes and procedures for the mitigation of and response to incidents. Finally, low is the level of know-how in the cybersecurity sector

owing to the shortage of experts with competences adequate to the management of information systems (ACN, 2023c, 2023d), the difficulties in attracting talents from within and outside the national labour market, as well as to the inadequate – if not absent – investments in the education of organisations' internal technical personnel (ACN, 2023a). On the other hand, the Global Cybersecurity Index published by the International Telecommunication Union (ITU) has alarmingly and repeatedly demonstrated how Italy's (especially technical) capabilities in cyberspace attain significantly inferior levels of maturity vis-à-vis other developed economies (ITU, 2021). Other studies have even reported that – notwithstanding its progresses in the field – in the past years, Italy's position in international rankings has considerably regressed, thus testifying to still insufficient effort and slowness in adopting more advanced cybersecurity measures (e-Governance Academy Foundation, 2023). Cognisant of the unviability of the current status quo, decision-makers within both the Italian public and private sectors have, hence, recently been more vocally calling for and adopting novel solutions and approaches to address their significant shortcomings in the field of cybersecurity and better tackle the risks and threats arising from the fifth domain.

Albeit with a notable delay in comparison to its allies and partners, over the past years, Italy has been increasingly recognising the criticality of constructing and maintaining a secure digital ecosystem and has consequently been accelerating its efforts to institutionalise a structured cybersecurity policy to be pursued through the definition of clear roles and responsibilities executed within a solid organisational architecture. Rome's 2022-2026 National Cybersecurity Strategy, in fact, not only complies with key international best practices and standards but also presents some elements of innovation. It revolves around the three major objectives of *protecting* national strategic assets through a systemic approach oriented to the management and mitigation of cyber risks, of *responding* to cyber threats, incidents and crises thanks to the pooling of all relevant stakeholders' capabilities of monitoring, detection,

analysis and reaction in the fifth domain, as well as that of encouraging a conscious and safe *development* of digital technologies, research and industrial competitiveness able to meet market demands. More specifically, the first strategic line of efforts ("protection") intends to implement measures, instruments and controls enabling and promoting a resilient digital transformation of the country. With this purpose, Italian authorities reckon as indispensable the strengthening of the capabilities of the National Assessment and Certification Centre (CVCN) and of its network of accredited laboratories to verify the absence of known vulnerabilities in information and communications technology (ICT) goods, systems and services, the definition and maintenance of an updated and coherent normative framework in the field of cybersecurity, the acquisition of more adequate technical instruments, sectorial competences and operational capabilities to enhance situational awareness on cyber threats, the boosting of the public sector's cyber maturity level, the development of the capabilities to protect national infrastructures and the promotion of the use of cryptography. The second set of actions delineated by Rome's cybersecurity strategic vision ("response") concerns, on the contrary, the post-cyber incident phase. Through the institutionalisation of a national and transnational cyber management system founded upon consolidated procedures of collaboration and information-sharing among key stakeholders, the organisation of periodic cyber exercises, the definition of the national posture and procedure with regard to cyber attribution and the countering of cybercrime, these initiatives are designed to allow the timeliest and most resolved reaction possible to cyber hostile behaviours. The third and final strategic objective ("development") synthetises the first two in a longer term perspective by highlighting the necessity to acquire a major autonomy in the cybersecurity field, as well as to lead innovation (ACN, 2023b) through increased investments and cooperation (ACN, 2022c).

More importantly, in its programmatic document, Rome has renovated the call for a radical paradigm shift and, in particular, for the urgency of

combining practices of cyber resilience and due diligence with tactics of active defence seeking to anticipate, prevent and mitigate cyber incidents also by augmenting the costs that cyber adversaries would need to bear in order to engage in hostile activities. Italian authorities have, hence, emphasised the primary importance of an efficient mechanism of cyber threat and crises management allowing, through the support of all relevant stakeholders, to predetermine possible cyber threat scenarios and perform the activities – ranging from their pre-alert to the very handling of their initial phases – necessary to thwart them (ACN, 2022c). In reality, in a series of governmental documents, over the past decade, Rome had already stressed the imperative of anticipating and preventing adverse COs against IT infrastructures and of thus ensuring the continuous delivery of the services depending on them. As an illustration, in December 2013, Italy published its first National Strategic Framework for Cyber Space Security and the related National Plan for Cyber Protection and ICT Security. The documents delineated a strategic and operational blueprint as well as the related practices considered essential for guaranteeing a secure digital space. Key priority was attributed to the development of the Italian intelligence agencies, law enforcement, as well as civilian and military defence forces' capabilities in the fifth domain. In this regard, the then Enrico Letta's Cabinet reiterated how the defence and security of networks and systems entail an in-depth understanding of the vulnerabilities, be them related to technological and/or human factors, and of the cyber threats exploiting them. More specifically, the above-mentioned institutional authorities were firstly called to enhance their capabilities in periodically analysing vulnerabilities and threats, monitoring technological innovations in all sectors dependent on the use of ICT systems and platforms with the intent of precociously identifying vulnerability profiles, sharing assessments with authorities responsible for key infrastructures, as well as in the collaboration with public and private research centres to elaborate avant-garde methodologies and technologies to detect possible weaknesses and threats. Secondly, they were

urged to boost their capabilities in gathering, elaborating and disseminating CYBINT, develop capabilities and procedures of knowledge management (i.e., the monitoring and correlation of information in order to promptly spot possible anomalies) and to implement early warning systems. Third and final worth-mentioning area for which ameliorations were recommended was represented by the capabilities of resisting threats, in particular through the enhancement of the ability to attribute cyberattacks, acquire cyber situational awareness and to favour agreements on information-sharing (Sistema di Informazione per la Sicurezza della Repubblica, 2013a, 2013b, 2017). Such initial yet promising attempts to define, at least on paper, a standardised process seeking to anticipate and not merely respond to malicious cyber scenarios have, however, not only not been pursued but they have also been dismissed by the directives ratified over the succeeding legislatures. Notwithstanding the approval of institutional architecture and governance reforms and/or the consolidation of some best practices, such acts as the Directive on cyber protection and national IT security or the Directive containing guidelines for cyber protection and national IT security (Gazzetta Ufficiale, 2017), respectively approved by the Matteo Renzi's Cabinet in August 2015 and the Paolo Gentiloni's one in February 2017, followed, in fact, the reactionary approach focused on the management of cyber crises rather than on their forecasting and prevention that had been previously designed by the Directive containing guidelines for national cybersecurity (Monti Decree) of January 2013 (Gazzetta Ufficiale, 2013).

The renewed acknowledgement of the criticality of adopting tactics of active cyber defence and the relative rapidity with which governance apparatuses have been instituted and reorganised also for these purposes have astonished numerous observers. The establishment of the Italian National Cybersecurity Agency (ACN) (Gazzetta Ufficiale, 2021a, 2021b) has, in fact, reformed the preceding politico-administrative architecture often paralysed by the presence of multiple decision-making centres and fragmented political responsibilities, as well as by a line of action that left ample margin of

manoeuvre to single entities and that lacked a precise coordinating structure. The most recent reform of the Italian national architecture of cybersecurity has rationalised the latter's governance and has remarkably raised security standards in order to meet those set at the European and international level, even with regard to cyber incidents prediction and prevention. More precisely, the ACN's Operations Service is currently articulated into the three following structures having, among others, proactive functions: the Italian Computer Security Incident Response Team (CSIRT), the Cyber Monitoring and Analysis centre and the National Risk Management, Cyber Capabilities and Collaborations unit (www.acn.gov.it). The first is responsible, *inter alia*, for monitoring national cyber events, issuing alerts and information concerning possible risks, analysing risks and threats and for performing activities oriented to increasing situational awareness (Gazzetta Ufficiale, 2018, 2019; www.csirt.gov.it). The second monitors public and private actors' level of exposure to digital threats through the conduction of cyber threat intelligence and early warning activities. The third complements the functions of the previous structure by specifically assessing cyber risk levels of strategic sectors and critical national infrastructures, developing models for estimating the potential impact of vulnerabilities and incidents, as well as by conducting statistical research on trends in the cyber threat landscape (www.acn.gov.it). Furthermore, within the Agency, the National Cybersecurity Nucleus operates to support the President of the Council of Ministers' decision-making concerning the activation of warning procedures and the prevention of and preparation for possible crisis situations. It has been redefined to act as primary and crucial forum for inter-ministerial coordination at a technical and operational level allowing, thanks to agile procedures of information-sharing, the synchronisation of cyber resilience and CYBINT activities (www.acn.gov.it). In sum, Italy has been moving significant steps towards the enhancement of its predictive power in cyberspace and, against the backdrop of the growing cyber risks aroused from the Russo-Ukrainian war, has recently demonstrated its increased capabilities. As a

consequence of the recent intensification of geopolitical tensions and the subsequent outburst of the conflict between Russia and Ukraine, the Agency and the National Anti-Crime Computer Centre for the Protection of Critical Infrastructures (CNAIPIC) have respectively issued over 19.500 (in the period comprised between 26 February and 29 March 2022) and 70 alerts (as of October 2022) concerning threats and vulnerabilities related to the ongoing conflict to entities encompassed within the National Cybersecurity Perimeter and national critical infrastructures. As further illustration, the Italian Postal and Communications Police Service has been boosting its network monitoring activities, not least by activating dedicated channels of direct dialogue with the Federal Bureau of Investigation (FBI), Europol and Interpol (ACN, 2023a; CLUSIT, 2023).

Positive are, moreover, the recent advancements made towards the implementation of two of the Cyber National Services outlined by the National Cybersecurity Strategy Implementation Plan. More specifically, Italy is committed to establishing a HyperSOC able to gather, correlate and analyse data – not only those already available to the Agency through its own activities or partnerships but also those deriving from accredited external parties – with the objective of guaranteeing the monitoring of both the constituency and relevant cyber threats. Such service is considered fundamental as it would permit the ACN to adopt preventive measures seeking, through the sharing of information on vulnerabilities and threats, to reduce the risk profiles of assets encompassed within the constituency, as well as to acquire increased situational awareness on the national cyber landscape. As a complement to such activities, Rome additionally intends to set up, under the directory of the ACN, a central Information Sharing and Analysis Centre (ISAC) integrable with a network of similar sectorial centres. The ISAC is devised to develop and distribute among key stakeholders strategic reports specific to the various sectors, as well as to more generally enhance the sharing of such added-value information as best practices, guidelines and recommendations (ACN, 2022b, 2023a). At present

the two Services still remain inactive but the ACN has defined and formalised their operational models and processes, as well as the requirements for the technological platforms supporting their provision (ACN, 2023a).

Notwithstanding the described key advancements (ACN, 2022a, 2023a) that Rome has recently made with the objective of increasing national levels of cybersecurity also by attempting to forecast and prevent cyber crisis scenarios, considerable deficiencies persist, however, in comparison to Washington's efforts in this regard. Among more systemic shortcomings is the one concerning the dynamic public-private partnership geared towards a "whole-of-nation" approach that has been set as overarching principle informing national efforts along the three strategic lines of action detailed above ("protection", "response" and "development"). Similarly to the United States and other partners, Italy has, in fact, repeatedly emphasised how the establishment of synergies with the private sector is critical for preventing and countering cyber threats (ACN, 2022c, Matassa, 2022). Over the past years, the ACN has thus attempted to formalise such collaboration also by stipulating memoranda of understanding and agreements through which the parties purport to share information and expertise (ACN, 2023a). In this regard, Rome has, nonetheless, yet to acknowledge a key issue that Washington contrarily seeks to address. The American National Cybersecurity Strategy recently published by President Joe Biden's Administration has surely benefitted from the policies undertaken in the previous decades, as well as from the assessment of their successes and failures. Whilst pursuing such efforts, some experts have yet observed and welcomed a concomitant relative deviation from past perspectives and practices. In particular, pivotal innovation is the administration's intent to foster a reconsideration of the cybersecurity responsibilities among the various national stakeholders. The White House has noted, in fact, that – despite having a significant role in ensuring a secure digital ecosystem – individuals, small businesses, infrastructure operators, as well as state and local governments bear a burden for reducing cyber risks and threats that is not commensurate with their

limited resources. The strategy thus seeks to forge a more effective and equitable public-private partnership that is conceived of as essential for reducing the harms caused by cyber threats to most vulnerable entities. As per the Biden's Administration, the federal government surely needs to enhance its leading and coordinating role in cyber-related matters. Nevertheless, the White House judges that increased roles and responsibilities should be allocated especially to the owners and operators of critical systems, as well as to the technology providers on which the latter depend. More specifically, in order to hold the (private) actors directly engaged in the provision of IT-based products and key services accountable also for guaranteeing their security and reliability, Washington intends to approve severer regulations (White House, 2023; Lewis, Walden and Neuberger, 2023; Lin, 2023; Harding, 2023). In this regard, the document states that "today's marketplace insufficiently rewards — and often disadvantages — the owners and operators of critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cyber incidents" (White House, 2023). New and updated regulatory frameworks are deemed critical for correcting such market failures that incentivise vendors and suppliers to downgrade cybersecurity measures in the attempt of acquiring a competitive edge and that consequently undermine the efforts to defend American networks and systems (White House, 2023).

More generally, compared to American ones, Italian efforts towards proactive cybersecurity policies and practices evidently remain at their infancy. Anticipating cyber events and incidents is portrayed in Rome's strategic documents as a challenge to be faced, not as an objective *per se* to be pursued (ACN, 2022c). Italy has recognised the need to enhance national capabilities of cyber defence and intelligence by acquiring increased situational awareness on the digital space through the continuous monitoring and analysis of vulnerabilities, threats and attacks and the utilisation of Machine Learning (ML)-based tools (ACN, 2022b, 2022c). Yet, in view of the fact that CYBINT research and elaboration activities and the conduction of COs to monitor,

prevent and counter cyber threats fall within the remit of Italian security services, scarce are the data publicly available and consequently ever complex is assessing Italian forecasting capabilities in the fifth domain (ACN, 2022b). In contrast, with the purpose of disrupting and dismantling threat actors' activities in cyberspace, the American National Cybersecurity Strategy explicitly states that "[t]he Federal Government will increase the speed and scale of cyber threat intelligence sharing to proactively warn cyber defenders and notify victims when the government has information that an organisation is being actively targeted or may already be compromised". As it is further pointed out, "[Sector Risk Management Agencies] (SRMAs), in coordination with [the Cybersecurity and Infrastructure Security Agency] (CISA), law enforcement agencies and the [Cyber Threat Intelligence Integration Center] (CTIIC), will identify intelligence needs and priorities within their sector and develop processes to share warnings, technical indicators, threat context and other relevant information with both government and non-government partners" (White House, 2023). President Joe Biden's commitment in this sense appears to testify to its Administration's intent to resurrect an albeit moderated proposal of developing a Federal Intrusion Detection Network (FIDNet) or a similar centralised cyber early warning and monitoring system able to resist the criticisms and obstructions from the Congress, private industry and civil rights groups that, over the past decades, have frustrated the Executive Branch's efforts to implement the initiative (Fuller, 2003). No other evident mention to Washington's intent and efforts to encourage the implementation of cyber prediction practices and models in both public and private sector entities is made in the document. Yet, the 2023-2025 CISA Strategic Plan provides more details in this regard. In addition to those of promoting both a whole-of-nation operational collaboration and the unification of the Agency, the scheme is in fact centred on the pillars of cyber defence and risk reduction and resilience. The first highlights CISA's commitment to continually innovate its threat hunting and vulnerability disclosure capabilities in order to enhance transparency into

national networks and systems. The second explains how the Agency utilises National Critical Functions (NCFs) to identify and anticipate risks to critical infrastructures and accordingly direct efforts to mitigate them, as well as how it will recur to analytical methodologies to guide its decision-making (CISA, 2022; Lewis *et al.*, 2022).

Moreover, the level of implementation of the various promising initiatives, measures and practices delineated by Rome is generally low within central government bodies and, *a fortiori*, the less-resourced sub-governmental entities and small- and medium-sized enterprises (SMEs). Particularly worrisome is the negligence towards official recommendations and requirements and the consequent low level of cybersecurity demonstrated by the Società Generale d'Informatica (Sogei) as it has serious impacts on the quality of information technology (IT) services of various Italian public administrations of which the organisation is the provider. Sogei has established a Security Operations Centre (SOC) that identifies, analyses, monitors and manages events of cybersecurity detected along its infrastructural perimeter. The organisation has a relatively distinct visibility into its IT environment thanks to the automated execution of vulnerability scans on the totality of its assets, the integration of an elevated number of information sources within its Security Information and Event Management (SIEM) platform and the utilisation of customised dashboards on the latter to visualise security alerts in real time. Within the organisation, a Computer Emergency Response Team (CERT) has additionally been activated for conducting, *inter alia*, Cyber Threat Intelligence (CTI) activities. Nonetheless, the Team has no access to the SIEM platform to perform its functions, does not carry out advanced analyses on security alerts and it remains unclear whether it is engaged in cyber warning intelligence activities. Processes, roles and responsibilities have not been defined, collaboration among the various structures is scarce and technological solutions or practices key for predicting and preventing cyber malevolent operations are lacking or inadequate (www.sogei.it). Fortunately more optimistic is, in contrast, the picture from

Italian larger companies. Following in their American and other international counterparts' footsteps, Italian large enterprises have been developing, in fact, a major cognisance of the criticality of cyber incidents prediction and prevention and have been adopting the necessary measures well in advance in comparison to public bodies. Similarly to what illustrated above, researchers have underlined how digital violations recorded by Italian (and American) enterprises are primarily to be ascribed to the fragility of their cybersecurity processes and the absent upgrading of their security technology solutions. In the face of the growing number and sophistication of cyber malicious operations, private corporations have (or have announced to) enhanced, adapted and/or allocated more resources to their information technology policies. The study has, in fact, additionally revealed that slightly less than 50 percent of Chief Information Officers (CIOs), Chief Technology Officers (CTOs) and Chief Information Security Officers (CISOs) interviewed have concurred in the necessity of acquiring increased visibility into their organisations' digital infrastructures to prevent incidents, as well as of revising the conception of and practices followed to guarantee security in cyberspace (VMware Inc., 2021). It has been observed that "the private sector has long suffered the consequences of the attack and intrusion activity driven by pervasive vulnerability and has not had the luxury to wait for a formal conceptual theory to emerge that might shape an effective policy response to the problem" (JD Work, 2020). Major Italian corporations such as Enel, Eni or Leonardo have been leveraging intelligence-based methodologies to enhance situational awareness and anticipate cyber risks, threats and crises. Nevertheless, they acknowledge that they may not guarantee that these and other cybersecurity solutions implemented will be sufficient to prevent malevolent behaviours against their systems (Enel, 2018, 2023; www.eni.com; Eni S.p.A., 2022; www.cybersecurity.leornardo.com). Among the reasons behind such issue, noteworthy is the question of supply chain security which represents a particularly serious issue for Italy. The Italian economic landscape is, in fact, primarily constituted by small- and medium-

sized enterprises that do not have the organisational structure, financial and technological resources, as well as the specialised personnel needed to systematically implement – often neither proactive nor reactive – cybersecurity practices (Faggioli, 2023). Most of them are not even aware of the National Framework for Cybersecurity and Data Protection that – founded upon the major guidelines and standards developed in the field of information security – Italy has elaborated as operational tool to organise public and private organisations' cybersecurity processes (CIS Sapienza and CINI, 2019, 2021). Relatively high levels of cybersecurity among large corporations are not sufficient since the compromise of smaller companies' poorly-secured digital assets on which the latter rely may have serious impacts on them. In order to guarantee satisfactory levels of security in cyberspace, methodologies and practices of cyber warning intelligence must be consolidated among Italian major organisations and introduced along their entire supply chain.

Chapter Six

Guidelines for the Model Implementation

Founding one's cybersecurity upon an indications and warning (I&W) structure demands continuous yet reasonable efforts from the part of organisations (Brodi *et al.*, 2022). In light of the series of models that have already been elaborated, difficulties might arise less from their definition than from their customisation to a particular case and their actual enforcement. Yet, as it has repeatedly been emphasised, the accurate and systematic implementation of analytical models is the indispensable lasting phase and ultimate objective of the preceding efforts devoted to their devising for supporting the handling of a certain issue. The present section advances, therefore, a series of suggestions for actively adopting the cyber I&W paradigm illustrated in Chapter Three. As mentioned above, whilst providing guidelines for predicting and anticipating cyber incidents that are applicable to various contexts, the paradigm has specifically been devised around the Italian cybersecurity landscape as an analytical tool to be adopted by Italian public bodies and large- and medium-sized enterprises. In this regard, it is to be specified here that if on the one hand the implementation of such a common framework seeks to institutionalise best practices and processes to forecast malicious cyber events (some of which have already been recommended by Rome's official documentations but which are currently rarely followed), on the other hand it inevitably creates discrepancies at a national level. Italian major public and private entities have set up cybersecurity architectures that differ due to distinct strategic considerations and decisions taken in light of their equally peculiar organisational structures, financial and other constraints, functions, sectors of belonging and their relative cyber threat ecosystems. The model needs, therefore, to be contextualised to the specific

organisation purporting to implement it. In other words, the latter needs to adjust the instructions provided by the model according to its institutional or business profile, the threats declared to be associated with its specific sector, its dimensions and other features. Organisations must examine the set of activities in which the framework has originally been articulated, as well as the rationales justifying and the principles informing them. In so doing, they will be able to measure the degree of compliance of their current status with the model, distinguish among the already-enacted measures those that are in accordance with the latter's best practices and that thus should be enhanced and those that should contrarily be dismissed, as well as to accordingly set the most adequate course of action. Albeit essential for effectiveness and efficiency purposes, such efforts to mould the framework to a certain organisation might, nevertheless, generate considerable variations on the implementation of the model. On the other hand, the one proposed is a high-level paradigm that does not thoroughly detail its macro-areas and several might be the possible interpretations of the recommended methodology for performing the corresponding activities. In the attempt to reduce the risk of exacerbating the divide among Italian organisations in terms of cyber maturity, the latter are encouraged to adopt additional cyber warning intelligence measures not encompassed within the proposed framework and yet considered – on the basis of their needs and capabilities – beneficial for forecasting cyberattacks but are exhorted not to neglect any of those delineated since they represent the indispensable ones to acquire predictive power in the fifth domain.

Initial prerequisite for the application of any analytical framework is its rigorous communication and diffusion among all interested parties. With this regard, political and military authorities and senior managers have critical responsibilities. Cynthia M. Grabo correctly stresses how "[decision-]makers must recognise that warning cannot be issued with absolute certainty, even under the best of circumstances, but will always be an assessment of probabilities [and must] realise that they will usually have to accept judgments

which are less firm, or based on less hard evidence, than they would wish" (Grabo, 2015). Nevertheless, decision-makers are not mere final addresses of warning alerts. They must contrarily be active promoters of the urgency to implement more proactive cybersecurity policies. In this sense, positive is the recent Italian acknowledgment – at least in the experts debate – of the priority need for increased cyber awareness and competences among the leaders of national organisations. The latter must guarantee that the cyber I&W paradigm has efficiently been disseminated and is comprehended by the personnel responsible for its enforcement. To be effective, cyber warning intelligence practices must, in fact, be routinised. For such purposes, novel processes must be formalised and ordinary ones must be revised to allow the integration of the former with the latter. Yet, these endeavours might result particularly problematic for Italian organisations. As noted in the previous chapter, the latter's cybersecurity approaches are generally quasi-exclusively reactive, inward-looking and myopic. Italian major governmental bodies and private corporations have been observed concentrating their cybersecurity efforts on the response to and recovery from adversarial intrusions into their information technology (IT) infrastructures. In general, they have already implemented such security solutions as Security Information and Event Management (SIEM), ticketing system, Security Orchestration, Automation and Response (SOAR) platforms that have been depicted here as key instruments to collect and storage data relative to past incidents that might provide valuable predictive intelligence about possible future attacks. Nonetheless, their often inefficient use not only undermines the efforts to manage detected cybersecurity events and incidents but also overlooks the predictive potential offered by such technological tools. Organisations' reaction to digital breaches is rarely supported by intelligence information concerning previous attacks against their systems or those of other entities active in the same sector and detailing the identity of the perpetrator of the malevolent action, the latter's root cause or the expected timing of possible similar future events. Furthermore, marginal currently is the number of Italian

organisations that have a Threat Intelligence Platform (TIP) integrated with SIEM, ticketing system, SOAR and other technologies for the collection, storage, processing, analysis and sharing of data concerning cyber threats and upon which the Early Warning System (EWS) proposed in Chapter Three is recommended to be founded.

The above-mentioned technological solutions assisting the process of developing predictive judgments about possible future cyber adverse scenarios are commonly provided by IT vendors and might be customised to a specific business context with relative ease. In contrast, a more serious issue among both the Italian public and private sectors that has been emphasised by the present investigation is relative to the paucity of expert personnel with elevated competences in Cyber Threat Intelligence (CTI) and cyber-related matters more generally, as well as to the confused allocation of their respective roles and responsibilities. Within their cybersecurity architectures, Italian organisations must establish a dedicated Early Warning structure staffed with a variable yet adequate number of specially-trained personnel responsible for distributing accurate, precise, reliable, complete, relevant, timely, usable, tailored and predictive CTI among all interested parties. In this regard, Bilyana Lilly et al. note that "[t]he general effectiveness of techniques and models [integrating both technical and non-technical CTI]" – as are those recommended here – "highly depends on the type of organisation, its information environment, available data on cyber adversaries, available resources and analytical capacity". The authors specify, therefore, that "[t]o use this research in their daily defence operations, cyber defence teams would need to work with a multidisciplinary staff, including statisticians, econometricians, computer scientists, and even criminologists and ethnographers, who can perform the analyses and translate them into actionable deliverables for a cyber defence team" (Lilly *et al.*, 2021). Entities implementing the I&W framework are to determine, *inter alia*, whether to conduct the entire spectrum of activities recurring to internal personnel, entrust it to external parties or to opt for a hybrid management modality.

Regardless of the option chosen, organisations must ensure that CTI products have strategic, operational and tactic utility for their cybersecurity needs, reach all relevant recipients and are of easy consumption (Kotsias *et al.*, 2023).

Finally, the implementation process of the I&W framework must be monitored through the definition of Key Performance Indicators (KPIs) supervising advancements and possible shortcomings in the conduction of each of its activities. By merely responding to – rather than proactively anticipating and preventing – COs launched by malicious state actors and cyber criminals against their information systems, the (reactive) defence measures adopted by Italian organisations have been lagging behind the rapid evolution of the cyber threat landscape. As repeatedly stressed, the cyber warning intelligence high-profile paradigm proposed here seeks to turn the tide. Nevertheless, its constant monitoring and adjustment in light of varying circumstances both internal and external to organisations is imperative to guarantee its effectiveness in predicting and considerably limiting the number of cyber incidents.

Conclusion

The present research project has had the ambitious objective of attempting to address the question of how cybersecurity strategies currently adopted by public and private organisations might be revised in light of a constantly evolving and increasingly sophisticated cyber threat ecosystem that demands a radical paradigm shift not towards the enhancement of early detection of and reaction to cyber incidents but towards the acquisition of capabilities to forecast them. More specifically, the author has revived the Cold War-era concept and practices of indications and warning (I&W) intelligence advanced by the American security services to predict and avert hostile events and has attempted to contribute to that line of academic work that has more recently applied them to the cybersecurity context. Concurring with some experts, it has been argued that integrating I&W intelligence methodologies within one's extant cybersecurity structures is essential to limit one's exposure to cyber risks and threats. Nevertheless, a high-level paradigm synthesising the major strengths and addressing some of the shortcomings of previous predictive analytical frameworks has been proposed here in order to lead as well as to enhance the effectiveness and efficiency of organisations' efforts to anticipate breaches into their information technology (IT) perimeter.

The absence of an authoritative definition of the concept of cyber I&W, the confidentiality of the issue and the overlapping of multiple levels of difficulty has rendered the designing of a cyber early-warning mechanism particularly complex. Moreover, it has been specified that the latter does not guarantee the prediction and prevention of all possible future cyberattacks that might target a certain organisation. Neither previous cybersecurity predictive models nor the one presented here are infallible methodologies recommending

equally infallible practices that ensure to shield organisations' IT perimeters against any possible malicious behaviour (Brodi, 1983). Denounced here is the generally scarce comprehension of and consequently illogical expectations on the function and objective of indications intelligence. Frequent – among decision-makers *in primis* – is, in fact, the conception that the intelligence community has and is called to have the omniscient capabilities of providing detailed forecasts of any hostile activity (Wirtz, 2013). Nevertheless, the present work has repeatedly emphasised how the prediction and prevention of malicious events especially in cyberspace is particularly complex owing to the latter's inherent opaqueness, the development of new and equally obscure technologies, as well as the expansion of both the circles of possible attackers and of the attack surface. As synthetised by James J. Wirtz, "[i]ndications and warning methodologies are based on key concepts and assumptions that must be understood and accepted by analysts and policymakers. Foremost among these assumptions is that indications and warning intelligence does not necessarily yield specific event predictions, only indications that the threat posed by some opponent is increasing". In other words, as the author further points out, "[i]f commanders or policy-makers insist on receiving specific details about what is about to transpire, or responses guaranteed to head off an attack, or compelling explanations for why an opponent is about to undertake an extremely counter-productive initiative, then warnings are likely to yield few positive results" (Wirtz, 2013). Daniel Gressang similarly maintains that, "[g]iven limitations in data access, target denial and deception activities, incomplete and at times contradictory data, significant time pressures and decision-maker perceptions and proclivities, […] [w]arning is imperfect" (Gressang, 2022).

Absolute cybersecurity is, on the other hand, an unattainable ideal. In view of the constant evolution and increasing sophistication of cyber threats, no IT system is today invulnerable and prediction strategies are not a panacea in cyberspace. Yet, if conducted according to structured processes compliant with relevant best practices having proven effectiveness, they are the solid

foundations upon which organisations' cybersecurity efforts to identify, prepare for, detect, respond to and recover from cyber incidents are to be constructed. The absence of an effective cyber warning system not only deprives defenders of the situational awareness of their respective perimeter of security and threat landscape necessary to anticipate malevolent cyber operations against their IT infrastructure, but it also nullifies the financial and other efforts expended in enhancing their (reactive) cybersecurity. Cognisant of the promises offered by the integration of intelligence methodologies within cyberspace and the opposite inadequacy of current cyber defence mechanisms, the author of the present work has observed that major public and private organisations have gradually been transitioning towards adopting more proactive measures. The research has focused here on the Italian case and has revealed some optimistic advancements in this sense. Yet, especially if juxtaposed to those devoted by their American counterparts, efforts by Italian large- and medium-sized enterprises and, *a fortiori*, governmental entities remain timid.

In light of the growing unrest and instability that dictate interactions in the fifth domain, the present research project has suggested a more viable approach able to handle cyber risks and enhance security whilst eschewing the potentially escalatory offensive capabilities that Rome and its international counterparts have commenced deploying to defend cyberspace (Gazzetta Ufficiale, 2022a, 2022b), as well as departing from merely reactionary measures that also private enterprises have predominantly been adopting. Nevertheless, numerous are the avenues for further investigation that remain open. More precisely, it might be of interest to analyse how the I&W paradigm proposed here or related methods might be adapted for small enterprise contexts. Their strategic value especially within the Italian economic system is directly proportional to the probability that they will be targeted by malevolent cyber operations with major frequency. Yet, a still scarce awareness of cyber risks and/or a paucity of resources are key issues justifying why such a truism does not always translate into increased focus on and investments in adequate

cybersecurity practices. In a similar manner, additional lines of study might move towards the application of I&W to specific sectors observed as majorly vulnerable to cyber threats or to other national environments. Nonetheless, of utter priority is the very promotion of such concept and practices. Despite their development in the bipolar period and their verified effectiveness, as well as the scholars, sectorial experts and policy-makers' calls to proactive, intelligence-led cybersecurity mechanisms raised over the past decades, their still scarce diffusion has consequential implications for the security of public and private digital assets.

Bibliography

Aarness, A. (2023) 'What is Endpoint Detection and Response (EDR)?', CrowdStrike, 6 February.

Abdlhamed, M. *et al.* (2017) 'Intrusion Prediction Systems', in I. M. Alsmadi *et al.* (eds.) Information Fusion for Cyber-Security Analytics. Studies in Computational Intelligence, Volume 691, Cham, Switzerland: Springer.

Agenzia per la Cybersicurezza nazionale (ACN) (2022a) '2021 Relazione annuale al Parlamento'. Available at: https://www.acn.gov.it/documents/ACN_Rel_Parlamento_2021.pdf. Accessed on 8th July 2023.

Agenzia per la Cybersicurezza nazionale (ACN) (2022b) 'Piano di implementazione Strategia Nazionale di Cybersicurezza 2022-2026'. Available at: https://www.acn.gov.it/ACN_Implementazione.pdf. Accessed on 25th May 2023.

Agenzia per la Cybersicurezza nazionale (ACN) (2022c) 'Strategia Nazionale di Cybersicurezza 2022-2026'. Available at https://www.acn.gov.it/ACN_Strategia.pdf. Accessed on 8th July 2023.

Agenzia per la Cybersicurezza nazionale (ACN) (2023a) '2022 Relazione annuale al Parlamento'. Available at: https://www.acn.gov.it/documents/ACN_Relazione_2022.pdf. Accessed on 8th July 2023.

Agenzia per la Cybersicurezza nazionale (ACN) (2023b) 'Agenda di ricerca e innovazione per la cybersicurezza 2023-2026'. Available at:

https://www.acn.gov.it/documents/agenda/it/ACN_ResearchInnovationAgenda.pdf. Accessed on 7th July 2023.

Agenzia per la Cybersicurezza nazionale (ACN) (2023c) 'Firmato l'accordo di collaborazione tra ACN e CRUI', 23 June.

Agenzia per la Cybersicurezza nazionale (ACN) (2023d) 'Frattasi: competenze digitali sin dalle elementari e nuova consapevolezza nella cybersecurity', 20 June.

Agenzia per la Cybersicurezza nazionale (ACN) (2023e) 'Strategia Nazionale di Cybersicurezza 2022-2026'. Available at: https://www.acn.gov.it/ACN_Strategia.pdf. Accessed on 25th May 2023.

Agenzia per la Cybersicurezza nazionale (ACN), 'Comitato interministeriale in materia di cybersicurezza'. Available at https://www.acn.gov.it/agenzia/coordinamento-interministeriale. Accessed on 25th May 2023.

Agenzia per la Cybersicurezza Nazionale (ACN), 'Operations'. Available at: https://www.acn.gov.it/en/agenzia/attivita/operazioni. Accessed on 17th June 2023.

Ahlm, E. (2021) 'How to Build and Operate a Modern Security Operations Center', Gartner, 7 June.

Ahmed, A. A. and Zaman, N. A. K. (2017) 'Attack Intention Recognition: A Review', International Journal of Network Security, Volume 19, Number 2, p.244-250.

Allen, G. and Chan, T. (2017) 'Artificial Intelligence and National Security', Belfer Center for Science and International Affairs, Harvard Kennedy School.

Aradau, C. and Blanke, T. (2015) 'The (Big) Data-security assemblage: Knowledge and critique', Big Data & Society, Volume 2, Number 2, p.1-12.

Arquilla, J. (2012a) 'Cool War. Could the Age of Cyberwarfare Lead Us to a Brighter Future?', Foreign Policy, 15 June.

Arquilla, J. (2012b) 'Cyberwar Is Already Upon Us. But Can It Be Controlled?', Foreign Policy, 27 February.

Arquilla, J. (2013) 'Twenty Years of Cyberwar', Journal of Military Ethics, Volume 12, Number 1, p.80-87.

Arquilla, J. and Ronfeldt, D. (1993) 'Cyberwar Is Coming!', reprinted in In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica, USA: RAND Corporation.

Associazione Italiana per la Sicurezza Informatica (CLUSIT) (2022) 'Rapporto Clusit 2022'. Available at: https://clusit.it/wp-content/uploads/download/Rapporto-Clusit-ottobre-2022_web.pdf. Accessed on 7th June 2023.

Associazione Italiana per la Sicurezza Informatica (CLUSIT) (2023) 'Rapporto Clusit 2023'. Available at: https://clusit.it/rapporto-clusit/. Accessed on 7th June 2023.

Baker, K. (2023) 'What is Cyber Threat Intelligence?', CrowdStrike, 23 March.

Banham, R. (2018) 'Using AI and Machine Learning to Anticipate Cyber Threats', Dell, 31 January.

Bejtlich, R. (2014) 'Strategy, Not Speed: What Today's Digital Defenders Must Learn From Cybersecurity's Early Thinkers', Brookings.

Bellasio, J. *et al.* (2020a) 'How could technological developments influence the future of cybercrime?', Santa Monica, USA: RAND Corporation.

Bellasio, J. e*t al.* (2020b) 'The Future of Cybercrime in Light of Technology Developments. Santa Monica, USA: RAND Corporation.

Bellovin, S. M. *et al.* (2017) 'Limiting the undesired impact of cyber weapons: technical requirements and policy implications', Journal of Cybersecurity, Volume 3, Number 1, p.59–68.

Björck, F. *et al.* (2015) 'Cyber Resilience – Fundamentals for a Definition', in Álvaro Rocha, Ana Maria Correia, Sandra Costanzo and Luís Paulo Reis (eds.) New Contributions in Information Systems and Technologies, Volume 1, Advances in Intelligent Systems and Computing, Volume 353, p.311-316, Cham, Switzerland: Springer.

Bonfanti, M. E. (2018) 'Cyber Intelligence: In Pursuit of a Better Understanding for an Emerging Practice', Cyber, Intelligence and Security, Volume 2, Number 1, p.105-121.

Borghard, E. D. and Lonergan, S. W. (2016) 'Can States Calculate the Risks of Using Cyber Proxies?', Orbis, Volume 60, Number 3, p.395-416.

Borum, R. *et al.* (2014) 'Cyber Intelligence Operations: More Than Just Ones and Zeros', Proceedings of the Marine Safety and Security Council: The US Coast Guard Journal of Safety and Security at Sea, Volume 71, Number 4, p.65-68.

Borum, R. *et al.* (2015) 'Strategic Cyber Intelligence', Information and Computer Security, Volume 23, Number 3, p.317-332.

Bou-Harb, E. *et al.* (2014) 'Cyber Scanning: A Comprehensive Survey', IEEE Communications Surveys & Tutorials, Volume 16, Number 3, p.1496-1519.

Brantly, A. F. (2014) 'Cyber Actions by State Actors: Motivation and Utility', International Journal of Intelligence and Counter-Intelligence, Volume 27, Number 3, p.465-484.

Brantly, A. F. (2018a) 'The Cyber Deterrence Problem', 2018 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects.

Brantly, A. F. (2018b) 'When everything becomes intelligence: machine learning and the connected world', Intelligence and National Security, Volume 33, Number 4, p.562-573.

Brantly, A. F. *et al.* (2016) 'The Motivation and Utility for Covert Action. In The Decision to Attack: Military and Intelligence Cyber Decision-Making', Athens, USA: University of Georgia Press.

Brodi, K. e*t al.* (2022) 'Planning for Significant Cyber Incidents: An Introduction for Decisionmakers', Santa Monica, USA: RAND Corporation.

Brody, R. (1983) 'The Limits of Warning', Washington Quarterly, Volume 6, Number 3, p.40-48.

Bucci, S. (2012) 'Joining Cybercrime and Cyberterrorism: A Likely Scenario' in Derek S. Reveron (ed.) Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World, Washington, DC, USA: Georgetown University Press.

Buchanan, B. (2017) 'The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations', New York, USA: Oxford University Press.

Caligiuri, M. and Pili, G. (2021) 'Italian Intelligence Studies Literature – Understanding the State of Play – A Comparative Perspective', The International Journal of Intelligence, Security and Public Affairs, Volume 23, Number 3, p.281-309.

Caltagirone, S. *et al.* (2013) 'The Diamond Model of Intrusion Analysis', United States Department of Defense, 7 May.

Cassetto, O. (2023) 'MITRE ATT&CK Explainers", Exebam. Available at: https://www.exabeam.com/explainers/mitre-attck/what-is-mitre-attck-an-explainer/. Accessed on 15 May 2023.

Check Point, 'Intrusion Detection System (IDS)'. Available at: https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/. Accessed on 13th June 2023.

Check Point, 'What is Vulnerability Scanning?'. Available at: https://www.checkpoint.com/cyber-hub/network-security/what-is-vulnerability-scanning/. Accessed on 20th June 2023.

Cisco, 'What Is a Firewall?'. Availbale at: https://www.cisco.com/c/en/us/products/security/firewalls/ what-is-a-firewall.html. Accessed on 11th June 2023.

Cisco, 'What Is Endpoint Security'. Available at: https://www.cisco.com/c/en/us/products/security/endpoint-security/index.html. Accessed on 13th June 2023.

Clausen, D. (2010) 'Coping with Bounds in the Debate over Japanese Defence: Analytical Eclecticism, Nonlinearity and the Lockwood Method: An Extended Literature Review and Methodological Review', LAMP-Method.org. Accessed 21/05/2023. URL http://lamp-method.org/eCommons/clausenLAMPmethods.pdf.

Computer Security Incident Response Team – Italia. Available at: https://www.csirt.gov.it/. Accessed on 17th June 2023.

Conti, M. *et al.* (2018) 'Cyber Threat Intelligence: Challenges and Opportunities', in Cyber Threat Intelligence. Advances in Information Security, Volume 70. Cham, Switzerland: Springer.

Cortex, 'What is a Threat Intelligence Platform'. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-threat-intelligence-platform. Accessed on 15th July 2023.

Council on Foreign Relations, 'Cyber Operations Tracker'. Available at: https://www.cfr.org/cyber-operations/. Accessed on 15th July 2023.

Craig, A. and Valeriano, B. (2016) 'Conceptualising cyber arms races', 2016 8th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, p.141-158.

CrowdStrike (2022) 'Indicators of Compromise (IoC) Security', 5 October. Available at: https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/. Accessed on 15th July 2023.

CrowdStrike (2023), 'Purple Teaming Explained', 24 February. Available at: https://www.crowdstrike.com/cybersecurity-101/purple-teaming/. Accessed on 15th July 2023.

Cybersecurity and Infrastructure Security Agency (CISA) (2022) 'CISA Strategic Plan 2023-2025', 1 September.

Cybersecurity and Infrastructure Security Agency (CISA), 'China Cyber Threat Overview and Advisories'. Available at: https://www.cisa.gov/china. Accessed on 7th May 2023.

Cybersecurity and Infrastructure Security Agency (CISA), 'Iran Cyber Threat Overview and Advisories'. Available at: https://www.cisa.gov/iran. Accessed on 7th May 2023.

Cybersecurity and Infrastructure Security Agency (CISA), 'North Korea Cyber Threat Overview and Advisories'. Available at: https://www.cisa.gov/northkorea. Accessed on 7th May 2023.

Cybersecurity and Infrastructure Security Agency (CISA), 'Russia Cyber Threat Overview and Advisories'. Available at: https://www.cisa.gov/russia. Accessed on 7th May 2023.

Cybersecurity and Infrastructure Security Agency (CISA), 'Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure', 9 May.

Dalton, A. *et al.* (2017) 'Improving Cyberattack Predictions Through Information Foraging', 2017 IEEE International Conference on Big Data (BIGDATA), Boston, USA, p.4642-4647.

Das, S. *et al.* (2022) 'The Role of AI-ML Techniques in Cyber Security' in Jena Om Prakash, H.L. Gururaj, M.R. Pooja and S.P. Pavan Kumar (eds.), Methods, Implementation, and Application of Cyber Security Intelligence and Analytics, Chapter 3, p.35-51, Hershey, USA: Information Science Reference, IGI Global.

Davydoff, D. (2018) 'Rethinking the Intelligence Cycle for the Private Sector', ASIS International, 1 January.

Denning, D. E. (2009) 'Barriers to Entry: Are They Lower for Cyber Warfare?', IO Journal, April.

Denning, D. E. (2015) 'Rethinking the Cyber Domain and Deterrence', Joint Force Quarterly, Volume 77, p.8-15.

Department of Defense of the United States of America (DoD) (2013a) 'Cyberspace Operations, Joint Publication 3-12(R)', 5 February.

Department of Defense of the United States of America (DoD) (2013b) 'Joint Intelligence, Joint Publication 2-0', 22 October.

Department of Defense of the United States of America (DoD) (2020), 'Directive 3115.16: The Defense Warning Network', Washington, D.C., USA: U.S. Department of Defense, Incorporating Change 2, 10 August.

Dhake, B. *et al.* (2023) 'Stratification of Hacker Forums and Predicting Cyber Assaults for Proactive Cyber Threat Intelligence', 2023 2nd International

Conference on Paradigm Shifts in Communications Embedded Systems, Machine Learning and Signal Processing (PCEMS), Nagpur, India, p.1-6.

Diehl, P. F. (1998) 'The Dynamics of Enduring Rivalries', Chicago, USA: University of Illinois Press.

Dupont, A. (2003) 'Intelligence for the Twenty-First Century', Intelligence and National Security, Volume 18, Number 4, p.15-39.

E-Governance Academy Foundation (2023) 'National Cyber Security Index – Italy'. Version updated to 2 June.

Eldridge, C. *et al.* (2018) 'Fusing algorithms and analysts: open-source intelligence in the age of "Big Data"', Intelligence and National Security, Volume 33, Number 3, p.391-406.

Enel (2018) 'Cyber Security, nasce a Torino la Global Control Room', 9 November.

Enel (2023) 'Cyber Harbour: un nuovo polo d'eccellenza per la sicurezza informatica', 21 June.

Eni S.p.A. (2022) 'Annual Report 2022'. Availbale at: https://report.eni.com/annual-report-2022/en/servicepages/downloads/files/entire-eni-ar22.pdf. Accessed on 9th July 2023.

Eni S.p.A., "Main risks". Available at: https://www.eni.com/en-IT/investors/risk-management/main-risks.html. Accessed on 9th July 2023.

Ernst & Young (EY) (2014) 'Cyber Threat Intelligence: How to Get Ahead of Cybercrime', November.

European Union Agency for Cybersecurity (ENISA) (2023) 'Identifying Emerging Cyber Security Threats and Challenges for 2030', March.

Faggioli, G. (2023) 'Nunzia Ciardi (ACN): ‘Convivere con il rischio cyber imparando a gestirlo"', Cybersecurity360, 3 January.

Farwell. J. P. and Rohozinski, R. (2011) 'Stuxnet and the Future of Cyber War', Survival, Volume 53, Number 1, p.23-40.

Federal Security Service (FSB) (2014) 'The concept of the state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation', Number K1274, 12 December.

Fischerkeller, M. P. and Harknett, R. J. (2017) 'Deterrence is Not a Credible Strategy for Cyberspace', Orbis, Volume 61, Number 3, p.381–393.

FortiGuard Labs (2022) ‘Cyber Threat Predictions for 2023: An Annual Perspective by FortiGuard Labs’, Fortinet, 7 November.

Fortinet, 'Endpoint Security'. Availbale at: https://www.fortinet.com/resources/cyberglossary/what-is-endpoint-security. Accessed on 13th June 2023.

Fortinet, 'Indicators of Compromise (IoCs)'. Available at: https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise. Accessed on 13th June 2023.

Fortinet, 'Intrusion Detection System (IDS)'. Available at: https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system. Accessed on 13th June 2023.

Fortinet, 'What Is a Firewall?'. Available at: https://www.fortinet.com/resources/cyberglossary/firewall. Accessed on 11th June 2023.

Fortinet, 'What is Endpoint Detection and Response (EDR)?'. Available at: https://www.fortinet.com/resources/cyberglossary/what-is-edr. Accessed on 13th June 2023.

Fortinet, 'What Is Intrusion Prevention System? Definition and Types'. Available at: https://www.fortinet.com/resources/cyberglossary/what-is-an-ips. Accessed on 13th June 2023.

Fortinet, 'What is Vulnerability Assessment? Types, Tools and Processes'. Available at: https://www.fortinet.com/resources/cyberglossary/vulnerability-assessment. Accessed on 20th June 2023.

Fuller, B. (2003) 'Federal Intrusion Detection, Cyber Early Warning and the Federal Response', SANS Institute, 19 June.

Galinec, D. and Steingartner, W. (2017) 'Combining Cybersecurity and Cyber Defense to Achieve Cyber Resilience', 2017 IEEE 14th International Scientific Conference on Informatics, Poprad, Slovakia, p.87-93.

Gartin, J. W. (2019) 'The Future of Analysis', Studies in Intelligence, Volume 63, Number 2, Extracts.

Gartner, 'Endpoint Detection and Response (EDR) Solutions Reviews and Ratings'. Available at: https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions. Accessed on 13th June 2023.

Gartner, 'Intrusion Detection and Prevention Systems Reviews and Ratings'. Available at: https://www.gartner.com/reviews/market/intrusion-prevention-systems. Accessed on 13th June 2023.

Gazzetta Ufficiale della Repubblica Italiana (2013) 'Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013. Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale (13A02504)', (GU Serie Generale n.66 del 19-03-2013). Available at:

https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Accessed on 17th June 2023.

Gazzetta Ufficiale della Repubblica Italiana (2017) 'Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017. Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali' (17A 2655) (GU Serie Generale n.87 del 13-04-2017). Available at: https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Accessed on 17th June2023.

Gazzetta Ufficiale della Repubblica Italiana (2018) 'Decreto Legislativo 18 maggio 2018, n. 65. Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione' (18G00092) (GU Serie Generale n.132 del 09-06-2018). Available at: https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Accessed on 17th June2023.

Gazzetta Ufficiale della Repubblica Italiana (2019) 'Decreto del Presidente del Consiglio dei Ministri 8 agosto 2019 Disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team - CSIRT italiano' (19A06940) (GU Serie Generale n.262 del 08-11-2019). Available at: https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Accessed on 17th June2023.

Gazzetta Ufficiale della Repubblica Italiana (2021a) 'Decreto del Presidente del Consiglio dei Ministri 9 dicembre 2021, n. 223. Regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale' (21G00246) (GU Serie Generale n.306 del 27-12-2021 - Suppl. Ordinario n. 47). Available at: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/origi

nario?atto.dataPubblicazioneGazzetta=2021-12-27&atto.codiceRedazionale=21G00246. Accessed on 17th June 2023.

Gazzetta Ufficiale della Repubblica Italiana (2021b) 'Decreto-Legge 14 giugno 2021, n. 82. Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale' (21G00098) (GU Serie Generale n.140 del 14-06-2021). Available at: https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Accessed on 17th June 2023.

Gazzetta Ufficiale della Repubblica Italiana (2022a), Decreto-Legge 9 agosto 2022, n.225. Misure urgenti in materia di energia, emergenza idrica, politiche sociali e industriali. (22G00128) (GU n.185 del 9-8-2022). Available at: https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Accessed on 26th June 2023.

Gazzetta Ufficiale della Repubblica Italiana (2022b), Legge 21 settembre 2022, n.142. Conversione in legge, con modificazioni, del decreto-legge 9 agosto 2022, n. 115, recante misure urgenti in materia di energia, emergenza idrica, politiche sociali e industriali (22G00152) (GU n.221 del 21-9-2022). Available at: https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario. Accessed on 26th June 2023.

Gilli, A. and Gilli, M. (2019) 'Why China Has Not Caught Up Yet. Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage', International Security, Volume 43, Number 3, p.141-189.

Goertz, G. and Diehl, P. F. (1993) 'Enduring Rivalries: Theoretical Constructs and Empirical Patterns', International Studies Quarterly, Volume 37, Number 2, p.147-171.

Goodman, W. (2010) 'Cyber Deterrence: Tougher in Theory than in Practice?', Strategic Studies Quarterly, Volume 4, Number 3, p.102–35.

Grabo, C. (with Jan Goldman) (2015) Handbook of Warning Intelligence, Lanham, USA: Rowman & Littlefield Publishing Group, Inc.

Greenberg, A. (2022), 'Cyber Security Forecast 2023', Mandiant, 2 November.

Gressang, D. (2022) 'Expanding Warning: Anticipating Diffused Threats', International Journal of Intelligence and Counter-Intelligence, Volume 0, Number 0, p.1-26.

Hachigian, N. (2001) 'China's Cyber Strategy', Foreign Affairs, Volume 80, Number 2, p.118-133.

Harding, E. (2023) 'From Maybe-Secure to Responsible Security: The New National Cybersecurity Strategy', Center for Strategic and International Studies, 6 March.

Hare, N. and Coghill, P. (2016) 'The future of the intelligence analysis task', Intelligence and National Security, Volume 31, Number 6, p.858-870.

Harknett, R. J. and Smeets, M. (2020) 'Cyber Campaigns and Strategic Outcomes', Journal of Strategic Studies.

Hathaway, O. A. *et al*. (2012) 'The Law of Cyberattack', California Law Review, Volume 100, Number 4, p.827-885.

Healey, J. (2017) 'Cyber Deterrence Is Working – So Far', The Cypher Brief, 23 July.

Hennessey, S. (2017) 'Deterring Cyberattacks: How to Reduce Vulnerability', Foreign Affairs, Voume. 96, Number 6, p.39-46.

Hernández, A. *et al.* (2016) 'Security attack prediction based on user sentiment analysis of Twitter data', 2016 IEEE International Conference on Industrial Technology (ICIT), Taipei, Taiwan, p.610-617.

Herrington, L. and Aldrich, R. (2013) 'The Future of Cyber-Resilience in an Age of Global Complexity'. Politics, Volume 33, Number 4, p.299–310.

Hettema, H. (2021) 'Rationality constraints in cyber defense: Incident handling, attribution and cyber threat intelligence', Computers & Security, Volume 109, p.1-13.

Heuer, R. J. Jr. and Pherson, R. H. (2009) 'Structured Analytic Techniques for Intelligence Analysis', Washington, DC., USA: CQ Press.

Hollenberger, J. (2023) 'A Guide to Incident Response Plans, Playbooks and Policy', Fortinet, 02 May.

Hulnick, A. S. (2005) 'Indications and Warning for Homeland Security: Seeking a New Paradigm', International Journal of Intelligence and Counter-Intelligence, Volume 18, Number 4, p.593-608.

Hutchins, E. M. *et al.* (2011) 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains', in Lockheed Martin Corporation (ed.) Leading Issues in Information Warfare & Security Research, Number 1.

Iasiello, E. (2014) 'Is Cyber Deterrence an Illusory Course of Action?', Journal of Strategic Security, Volume 7, Number 1, p.54-67.

IBM (2021) 'Ticketing process'. Last updated on 3rd March. Accessed on 13th July 2023. Available at: https://www.ibm.com/docs/en/sss/3.1.1?topic=SSETBF_3.1.1/com.ibm.siteprotector.doc/concepts/sp_ticketing_process.htm.

IBM, 'Artificial Intelligence (AI) for Cybersecurity'. Available at: https://www.ibm.com/security/artificial-intelligence. Accessed on 15th July 2023.

IBM, 'Security Operations Center (SOC)'. Available at: https://www.ibm.com/topics/security-operations-center. Accessed on 08th June 2023.

IBM, 'What is Security Information and Event Management (SIEM)?'. Available at: https://www.ibm.com/topics/siem. Accessed on 13th June 2023.

Ibor, A.E. *et al.* (2020) 'Conceptualisation of Cyberattack prediction with deep learning'. Cybersecurity, Volume 3, Number 14.

Imperva, 'Vulnerability Assessment'. Available at: https://www.imperva.com/learn/application-security/vulnerability-assessment/. Accessed on 20th June 2023.

Information Security Forum (ISF) (2019) 'Building A Successful SOC: Detect Earlier, Respond Faster', April.

Intelligence and National Security Alliance (INSA) (2011) 'Cyber Intelligence: Setting the Landscape for an Emerging Discipline', September.

Intelligence and National Security Alliance (INSA) (2018) 'A Framework for Cyber Indications and Warning', October.

International Institute for Strategic Studies (IISS), 'Cyber Report'. Available at: https://www.iiss.org/online-analysis/cyber-report/. Accessed on 15th May 2023.

International Telecommunication Union (ITU) (2021) '2020 Global Cybersecurity Index'. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. Accessed on 8th July 2023.

Ish, D. *et al.* (2021) 'Evaluating the Effectiveness of Artificial Intelligence Systems in Intelligence Analysis', Santa Monica, USA: RAND Corporation.

Jamieson, K. H. (2018) 'Cyberwar: How Russian Hackers and Trolls Helped Elect a President', New York, USA: Oxford University Press.

JD Work (2020) 'Evaluating Commercial Cyber Intelligence Activity', International Journal of Intelligence and Counter-Intelligence, Volume 33, Number 2, p.278-308.

JD Work (2022) 'The First Purpose: Rediscovering Warning Analysis for CTI', SANS Institute, 28 January.

Jensen, E. T. (2012) 'Cyber Deterrence', Emory International Law Review, Volume 26, Number 2, p.773-824.

Kaminska, M. (2022) 'Cyber Operations During the 2022 Russian Invasion of Ukraine: Lessons Learned (So Far), European Cyber Conflict Research Initiative, Tallinn Workshopr Report, July.

Kaspersky Lab, 'Targeted Cyberattacks Logbook'. Available at: https://apt.securelist.com/. Accessed on 12th June 2023.

Kaspersky Lab, 'What is a firewall? Definition and explanation'. Available at: https://www.kaspersky.com/resource-center/definitions/firewall. Accessed on 11th June 2023.

Kello, L. (2017) 'The Virtual Weapon and International Order', New Haven, USA: Yale University Press.

Knake, R. K. (2019) 'Building Resilience in the Fifth Domain', Council on Foreign Relations, 16 July.

Kotsias, J. e*t al.* (2023) 'Adopting and integrating cyber-threat intelligence in a commercial organisation', European Journal of Information Systems, Volume 32, Number 1, p.35-51.

Kott, A. (2014) 'Towards Fundamental Science of Cyber Security', in Robinson E. Pino (ed.) Network Science and Cybersecurity, Volume 55, New York, USA: Springer.

Langø, H.(2016) 'Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security', in K. Friis and J. Ringsmose (eds.) Conflict in Cyber Space, London, UK: Routledge.

Laur, T. M. (1986) 'Principles of Warning Intelligence' in G. Hopple and B. Watson (eds.) The Military Intelligence Community, Chapter 11, New York, USA: Routledge.

Leau, Y. and Manickam, S. (2015) 'Network Security Situation Prediction: A Review and Discussion', in R. Intan *et al.* (eds.) Intelligence in the Era of Big Data. ICSIIT 2015. Communications in Computer and Information Science, Volume 516, Berlin, DE: Springer.

Lewis, J. A. (2019) 'Iran and Cyber Power', Center for Strategic and International Studies (CSIS), 25 June.

Lewis, J. A. (2019) 'Iran and Cyber Power', Center for Strategic and International Studies (CSIS), 29 June.

Lewis, J. A. (2022) 'CISA Strategic Plan for 2023-2025: The Future of U.S. Cyber and Infrastructure Security, Center for Strategic and International Studies (CSIS), 1 November. Available at: https://www.youtube.com/watch?v=PcjIh4adtAc, https://www.csis.org/analysis/cisa-strategic-plan-2023-2025-future-us-cyber-and-infrastructure-security.

Lewis, J. A. (2023) 'Cyber War and Ukraine', Center for Strategic and International Studies (CSIS), 16 June.

Lewis, J. A. and Wood, G. (2023) 'Evolving Cyber Operations and Capabilities', Center for Strategic and International Studies (CSIS), 18 March.

Lewis, J., A. *et al.* (2023) ‘The Biden-Harris Administration’s National Cybersecurity Strategy’, Center for Strategic and International Studies, 2 March.

Lieber, K. (2014) ‘The Offense-Defense Balance and Cyber Warfare’, in E. O. Goldman (ed.) Cyber Analogies, p.96-107, Monterey, USA: Naval Postgraduate School.

Lilli, E. (2021) 'Redefining deterrence in cyberspace: Private sector contribution to national strategies of cyber deterrence', Contemporary Security Policy, Volume 42, Number 2, p.163-188.

Lilly, B. *et al.* (2019) 'Applying Indications and Warning Frameworks to Cyber Incidents', in T. Minárik *et al.* (eds.), 11th International Conference on Cyber Conflict: Silent Battle, Proceedings 2019, Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Lilly, B. *et al.* (2021) 'RAND’s Scalable Warning and Resilience Model (SWARM): Enhancing Defenders’ Predictive Power in Cyberspace', Santa Monica, USA: RAND Corporation.

Lim, K. (2016) 'Big Data and Strategic Intelligence', Intelligence and National Security, Volume 31, Number 4, p.619-635.

Lin, H. (2012) 'Escalation Dynamics and Conflict Termination in Cyberspace', Strategic Studies Quarterly, Volume 6, Number 3, p.46-70.

Lin, H. (2023) 'Where the New National Cybersecurity Strategy Differs From Past Practice', Lawfare, 6 March.

Lindsay, J. R. (2015) 'The Impact of China on Cybersecurity. Fiction and Friction', International Security, Volume 39, Number 3, p.7-47.

Linkov, I. and Kott, A. (2019) 'Fundamental Concepts of Cyber Resilience: Introduction and Overview' in Cyber Resilience of Systems and Networks, Cham, Switzerland: Springer.

Lockheed Martin, 'Cyber Kill Chain'. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Accessed on 22nd May 2023.

Lockwood, J. (2002) 'The Lockwood Analytic Method for Prediction (LAMP): An Innovative Methodological Approach to the Problem of Predictive Analysis', 15 January.

Lockwood, J. (2010) 'The Application of LAMP'. Available at: http://lamp-method.org/2.html. Accessed on 21st May 2023.

Lucas, K. (2013) 'The Meaning of the Cyber Revolution. Perils to Theory and Statecraft', International Security, Volume 38, Number 2, p.7-40.

Maimon, D. *et al.* (2017) 'Re-Thinking Online Offenders' SKRAM: Individual Traits and Situational Motivations as Additional Risk Factors for Predicting Cyber Attacks', IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, 15th International Conference on Pervasive Intelligence and Computing, 3rd International Conference on Big Data Intelligence and Computing, and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Orlando, Fla., November 6–10, pp. 232-238.

Mandel, D. (2022) 'Communicating Uncertainty in Warning Intelligence, The Journal of Intelligence, Conflict and Warfare, Volume 4, Number 3, p.133-137. Presentation delivered at the 2021 Canadian Association for Security and Intelligence Studies (CASIS) West Coast Security Conference, 23 November 2021.

Mandiant, 'Targeted Attack Lifecycle'. Available at: https://www.mandiant.com/resources/insights/targeted-attack-lifecycle. Accessed on 23rd May 2023.

Maness, R. C. (2017a) 'Codebook for the Dyadic Cyber Incident and Dispute Data, Version 1.1'. Available at: https://a678132e-4067-4ed4-800a-239c80659fd1.filesusr.com/ugd/4b99a4_4c7971ea77914 64a8ac551fff85fb1f 1.pdf. Accessed on 17th November 2022.

Maness, R. C. (2017b) 'The Dyadic Cyber Incident and Dispute Dataset', Version 1.1. Available at: https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset. Accessed on 17th November 2022.

Maness, R. C. *et al.* (2019a) 'Codebook for the Dyadic Cyber Incident and Campaign Dataset (DCID) Version 1.5'. Available at: https://a678132e-4067-4ed4-800a-239c80659fd1.filesusr.com/ugd/4b99a4_f459cbee54c549ffbbd086963de94a 1c.pdf. Accessed on 17th November 2022.

Maness, R. C. *et al.* (2019b) 'The Dyadic Cyber Incident and Dispute Dataset', Version 1.5. Available at: https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset. Accessed on 17th November 2022.

Maness, R. C. *et al.* (forthcoming) 'Expanding the Dyadic Cyber Incident and Dispute (DCID) Dataset: Cyber Conflict', Cyber Defense Review.

Maness. R. C. and Valeriano, B. (2016) 'The Impact of Cyber Conflict on International Interactions', Armed Forces and Society, Volume 42, Number 2, p.301-323.

Martino, L. (2019) 'Spazio cibernetico: le minacce, i rischi e le opportunità per l'Italia', Centre for Cyber Security and International Relations Studies.

Martino, L. (2021) 'Geopolitics of Data: The Revenge of Geography in Cyberspace?', Italian Institute for International Political Studies (ISPI), 31 May.

Maschmeyer, L., *et al.* (2021) 'A tale of two cybers: how threat reporting by cybersecurity firms systematically underrepresents threats to civil society', Journal of Information Technology and Politics, Volume 18, Number 1, p.1-20.

Matassa, M. (2022) 'Una strategia nazionale a difesa del cyberspazio', P.A. Persona e Amministrazione, Università degli Studi di Urbino Carlo Bo, Volume 11, Number 2, p.625-653.

Maurer, T. and Hinck, G. (2018) 'Russia's Cyber Strategy', Italian Institute for International Political Studies (ISPI), 19 December.

Mavzer, K. B. *et al.* (2021) 'Trust and Quality Computation for Cyber Threat Intelligence Sharing Platforms', 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, p.360-365.

McMillan, R. (2010) 'Siemens: Stuxnet worm hit industrial systems', Computerworld, 14 September.

Microsoft, 'What is SIEM?'. Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem. Accessed on 13th July 2023.

Microsoft, 'What is SOAR?'. Available at: https://www.microsoft.com/en-us/security/business/security-101/what-is-soar. Accessed on 13th July 2023.

Minerva Research Initiative (2020) 'Automated Early Warning System for Cyber Intrusion', Richard Carley Selected for Research Award 2020 (2021-2023). Available at: https://minerva.defense.gov/Research/Funded-Projects/Article/2463597/automated-early-warning-system-for-cyber-intrusion/. Accessed on 13th July 2023.

Muller, L. P. and Stevens, T. (2017) 'Upholding the NATO cyber pledge. Cyber Deterrence and Resilience: Dilemmas in NATO defence and security politics', Norwegian Institute of International Affairs, Policy Brief 5/2017.

Nakashima, E. and Warrick, J. (2012) 'Stuxnet was work of U.S. and Israeli experts, officials say', The Washington Post, 2 June.

National Academies of Sciences, Engineering, and Medicine (2019) 'Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop', Washington, DC, USA: The National Academies Press.

National Institute of Standards and Technology (NIST) (2018) ‘Framework for Improving Critical Infrastructure Cybersecurity’, Version 1.1, 16 April.

National Institute of Standards and Technology (NIST) (2021) 'Managing Information Security Risk: Organization, Mission, and Information System View', Gaithersburg, USA: Joint Task Force Transformation Initiative, Special Publication 800-39, March.

Nussbaum, B. H. (2017) 'Communicating Cyber Intelligence to Non-Technical Customers', International Journal of Intelligence and Counter-Intelligence, Volume 30, Number 4, p.743-764.

Nye, J. S. (2010) 'Cyber Power', Belfer Center for Science and International Affairs, Harvard Kennedy School.

Nye, J. S. Jr. (2017) 'Deterrence and Dissuasion in Cyberspace', International Security, Volume 41, Number 3, p.44-71.

Nye, J. S. Yr. (2019) 'Rules of the Cyber Road for America and Russia', Project Syndicate, 5 March.

Office of the Director of National Intelligence (ODNI) (2023) 'Annual Threat Assessment of the U.S. Intelligence Community', 6 February.

Onoh, G. (2018) ‘Predicting Cyber-Attacks Using Publicly Available Data, Journal of the Colloquium for Information System Security Education (CISSE), Volume 6, Number 1, September.

Oosthoek, K. and Doerr, C. (2021) 'Cyber Threat Intelligence: A Product Without a Process?', International Journal of Intelligence and Counter-Intelligence, Volumd 34, Number 2, p.300-315.

Oracle, 'What is Big Data?'. Available at: https://www.oracle.com/big-data/what-is-big-data/. Accessed on 14th Juen 2023.

Orchilles, J. (2022) 'Shifting from Penetration Testing to Red Team and Purple Team', SANS Institute, 17 March.

Pace, C. (2018) 'The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence', Annapolis, USA: CyberEdge Group.

Palo Alto Networks, 'What is an Intrusion Prevention System?'. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips. Accessed on 13th June 2023.

Paloalto Networks, 'What is SOAR?'. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-soar. Accessed on 13th July 2023.

Panagiotou, P. *et al.* (2021) 'Towards Selecting Informative Content for Cyber Threat Intelligence', 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, p.354-359.

Papastergiou, S. *et al.* (2020) 'Cyber Security Incident Handling, Warning and Response System for the European Critical Information Infrastructures (CyberSANE)', Engineering Applications of Neural Networks, 20th

International Conference (EANN2019) Proceedings. Communications in Computer and Information Science, Volume 1000, p.476-487.

Parisi, A. (2019) 'Hands-On Artificial Intelligence for Cybersecurity: Implementing Smart AI Systems for Preventing Cyber Attacks and Detecting Threats and Network Anomalies', Birmingham, UK: Packt Publishing.

Parker, D. B. (1998) 'Fighting Computer Crime: A New Framework for Protecting Information', New York, USA: John Wiley & Sons.

Pöyhönen, J. *et al.* (2019), 'Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations', Information & Security: An International Journal, Volume 43, Number 2, p.236-256.

PricewaterhouseCoopers (PwC) (2023) 'Cyber Threats 2022: A Year in Retrospect'.

Rajamäki, J. and Katos, V. (2020), 'Information Sharing Models for Early Warning Systems of Cybersecurity Intelligence', Information & Security: An International Journal, Volume 46, Number 2, p.198-214.

Ramaki, A. A. and Atani, R. E. (2016) 'A survey of IT early warning systems: architectures, challenges and solutions', Security and Communication Networks, Volume 9, Number 17, p.4751-4776.

Rantos, K. et al. (2020) 'Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem', Computers, Volume 9, Number 1, 6 March, p.1-18.

Regens, J. L. (2019) 'Augmenting human cognition to enhance strategic, operational, and tactical intelligenc', Intelligence and National Security, Volume 34, Number 5, p.673-687.

Research Center of Cyber Intelligence and Information Security (CIS Sapienza) and CINI Cybersecurity National Laboratory (2016) '2015 Italian

Cyber Security Report: Un Framework Nazionale per la Cyber Security', Version 1.0, February.

Research Center of Cyber Intelligence and Information Security (CIS Sapienza) and CINI Cybersecurity National Laboratory (2017) '2016 Italian Cybersecurity Report: Cybersecurity Essential Controls', Version. 1.0., March.

Research Center of Cyber Intelligence and Information Security (CIS Sapienza) and CINI Cybersecurity National Laboratory (2019) 'Framework Nazionale per la Cybersecurity e la Data Protection', February.

Research Center of Cyber Intelligence and Information Security (CIS Sapienza) and CINI Cybersecurity National Laboratory (2021) 'Metodologia per il cybersecurity Assessment con il Framework Nazionale per la Cybersecurity e la Data Protection', Version 1.0, September.

Rid, T. (2012) 'Cyber War Will Not Take Place', Journal of Strategic Studies, Volume 35, Number 1, p.5-32.

Rid, T. (2013) 'Cyberwar and Peace: Hacking Can Reduce Real-World Violence', Foreign Affairs, Volume 92, Number 6, p.77-87.

Roberts, S. J. *et al.* (2017) 'Intelligence-Driven Incident Response: Outwitting the Adversary', Sebastopol, USA: Oreilly & Associates Inc.

Robinson, M. *et al.* (2012) 'Cyber Threat Indications and Warning: Predict, Identify and Counter', Small Wars Journal, 26 July.

Rugge, F. (2018) 'Confronting an "Axis of Cyber"?: China, Iran, North Korea, Russia in Cyberspace', Italian Institute for International Political Studies (ISPI), October.

Russell, A. L. (2017) 'The Physical Layer' in Strategic A2/AD in Cyberspace, Cambridge, UK: Cambridge University Press.

Sakuraba, T. *et al.* (2008) 'Exploring Security Countermeasures along the Attack Sequence', 2008 International Conference on Information Security and Assurance (ISA 2008), Busan, South Korea, p.427-432.

Saltzman, I. (2013) 'Cyber Posturing and the Offense-Defense Balance', Contemporary Security Policy, Volume 34, Number 1, 11 March, p. 40-63.

Samtani, S. *et al.* (2017) 'Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence', Journal of Management Information Systems, Volume 34, Number 4, p.1023-1053.

Scarfone, K. (2023) 'How to create an incident response playbook', TechTarget, March.

ServiceNow, 'What is an IT ticketing system?'. Available at: https://www.servicenow.com/products/itsm/what-is-it-ticketing-system.html. Accessed on 13th July 2023.

Shaheen, S. (2014) 'Offense-Defense Balance in Cyber Warfare' in JF. Kremer and B. Müller (eds.) Cyberspace and International Relations, Berlin, DE: Springer.

Shahriar, S. *et al.* (2022) 'A Review of Dark Web: Trends and Future Directions', 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC), p.1780-1785.

Shanchieh J. *et al.* (2014) 'Attack Projection' in A. Kott *et al.* (eds.) Cyber Defense and Situational Awareness, Volume 62, Chapter 11, p.239-261, Cham, Switzerland: Springer.

Sharma, A. *et al.* (2013) 'A Social Dimensional Cyber Threat Model with Formal Concept Analysis and Fact-Proposition Inference', University of Nebraska Omaha, Computer Science Faculty Publications, Number 24.

Shu, K. *et al.* (2018) 'Understanding Cyber Attack Behaviors with Sentiment Information on Social Media' in R. Thomson *et al.* (eds.) Social, Cultural, and Behavioral Modeling. 11th International Conference, SBP-BRiMS 2018, Volume 10899. Cham, Switzerland: Springer.

Siciliano, M. (2022) 'Introduzione' in Commissione di Studi Cyber Threat Intelligence e Cyber Warfare (ed.), Le prospettive della cyber intelligence, Società Italiana di Intelligence (SOCINT), Vol. 1, Arcavacata di Rende, ITA: Università della Calabria.

Singh, J. (2013) 'The Lockwood Analytical Method for Prediction within a Probabilistic Framework', Journal of Strategic Security, Volume 6, Number 3, p.83-99.

Sistema di Informazione per la sicurezza della Repubblica (2013a) 'Piano nazionale per la protezione cibernetica e la sicurezza informatica', Presidenza del Consiglio dei Ministri, December.

Sistema di Informazione per la sicurezza della Repubblica (2013b) 'Quadro strategico nazionale per la sicurezza dello spazio cibernetico', Presidenza del Consiglio dei Ministri, December.

Sistema di Informazione per la sicurezza della Repubblica (2017) 'Piano nazionale per la protezione cibernetica e la sicurezza informatica', Presidenza del Consiglio dei Ministri, March.

Sistema di Informazione per la Sicurezza della Repubblica (2022) 'Relazione Annuale sulla politica dell'informazione per la sicurezza 2021'.

Sistema di Informazione per la Sicurezza della Repubblica (2023) 'Relazione Annuale sulla politica dell'informazione per la sicurezza 2022'.

Slayton, R. (2017) ‘What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment’, International Security, Volume 41, Number 3, 1 January, p.72–109.

Smeets, M. (2018) 'The Strategic Promise of Offensive Cyber Operations', Strategic Studies Quarterly, Volume 12, Number 3, p.90-113.

Smeets, M. and Soesanto, S. (2020) 'Cyber Deterrence Is Dead. Long Live Cyber Deterrence!', Council on Foreign Relations, 18 February.

Smith, Z. L. M. (2022) 'Emerging Cyber Threats: No State Is an Island in Cyberspace', Center for Strategic and International Studies, 23 March.

Smythe, C. (2020) ‘Cult of the Cyber Offensive: Misperceptions of the Cyber Offense/Defense Balance’. Yale Journal of International Affairs, Volume 15, p.98-114.

Soesanto, S. (2022) 'Cyber Deterrence Revisited', Alabama, USA: Air University Press.

Soesanto, S. and Smeets, M. (2021) 'Cyber Deterrence: The Past, Present and Future' in F. Osinga and T Sweijs (eds.) Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century – Insights from Theory and Practice, The Hague, The Netherlands: T.M.C. Asser Press.

Strom, B. E. *et al.* (2020) 'MITRE ATT&CK®: Design and Philosophy', The MITRE Corporation.

Taddeo, M. and Floridi, L. (2018) 'Regulate artificial intelligence to avert cyber arms race', Nature, 16 April.

The MITRE Corporation, 'ATT&CK' (2015-2023). Available at: https://attack.mitre.org/. Accessed on 11th June 2023.

The Open Worldwide Application Security Project (OWASP), 'Vulnerability Scanning Tools'. Available at: https://owasp.org/www-community/Vulnerability_Scanning_Tools#. Accessed on 20th June 2023.

The Security Council of the Russian Federation (SCRF) (2016) 'Doctrine of Information Security of the Russian Federation', Number 646, 5 December.

The White House Office of the Press Secretary (2013) 'Presidential Policy Directive/PPD-21', 12 February.

Thomas, M. A. (2022) 'Distinguishing Cyberattacks by Difficulty', International Journal of Intelligence and Counter-Intelligence, Volume 35, Number 4, p.784-805.

Tor, U. (2017) '"Cumulative Deterrence" as a New Paradigm for Cyber Deterrence', Journal of Strategic Studies, Volume 40, Number 1-2, p.92-117.

Trellix, 'What is Stuxnet?'. Available at: https://www.trellix.com/en-gb/security-awareness/ransomware/what-is-stuxnet.html. Accessed on 30th April 2023.

Trost, R. W. (2023) 'Threat Intelligence Platform, SIEM or Ticketing System: What is the Difference?', Threat Quotient.

United States' Office of the Director of National Intelligence (ODNI) (2017) "Background to Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution', 6 January.

US Government (2009) 'A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis'. Accessed on 11th June 2023. Available at: https://www.cia.gov/static/955180a45afe3f5013772c313b16face/Tradecraft-Primer-apr09.pdf.

Valeriano, B. (2022a) 'Dyadic Cyber Incident Dataset v.2.0', Harvard Dataverse.

Valeriano, B. (2022b) ‘The Failure of Offense/Defense Balance in Cyber Security’, The Cyber Defense Review, Volume 7, Number 3, p.91-102.

Valeriano, B. and Maness, R. C. (2012) 'Persistent Enemies and Cyberwar. Rivalry Relations in an Age of Information Warfare' in D. S. Reveron (ed.) Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World, Washington, D.C., USA: Georgetown University Press.

Van Puyvelde, D. and Brantly, A. F. (2019) 'Cybersecurity. Politics, Governance and Conflict in Cyberspace', Cambridge: Polity Press.

Van Puyvelde, D. *et al.* (2017) 'Beyond the buzzword: big data and national security decision-making', International Affairs, Volume 93, Number 6, p.1397-1416.

VMware Inc. (2021) 'Report Security Insights di VMware per l’Italia'. Available at: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-global-security-insights -report-italy.pdf. Accessed on 7th June 2023.

Vogel, K. M. *et al.* (2021) 'The impact of AI on intelligence analysis: tackling issues of collaboration, algorithmic transparency, accountability, and management', Intelligence and National Security, Volume 36, Number 6, p.827-848.

Voo, J. *et al.* (2020) 'National Cyber Power Index 2020. Methodology and Analytical Considerations', Belfer Center for Science and International Affairs, Harvard Kennedy School.

Voo, J. *et al.* (2022) 'National Cyber Power Index 2022', Belfer Center for Science and International Affairs, Harvard Kennedy School.

Welburn, J. *et al.* (2023) 'Cyber deterrence with imperfect attribution and unverifiable signaling', European Journal of Operational Research, Volume 306, p.1399-1416.

Wenger, A. and Wilner, A. (2021) 'Deterrence by Denial: Theory and Practice', Amherst, USA: Cambria Press.

White House (2023) 'National Cybersecurity Strategy', March.

Wickes, C. (2021) 'In Data We Trust: Leveraging Large Scale Analytics for Intrusion Detection', SANS Institute, 30 November.

Williams, P. *et al.* (2002) 'Intelligence Analysis for Internet Security', Contemporary Security Policy, Volume 23, Number 2, p.1-38.

Wilner, A. (2017) 'Cyber deterrence and critical-infrastructure protection: Expectation, application and limitation', Comparative Strategy, Volume 36, Number 4, p.309-318.

Wirtz, J. J. (2013) 'Indications and Warning in an Age of Uncertainty', International Journal of Intelligence and Counter-intelligence, Volume 26, p.550–562.

Yucel, C. *et al.* (2020) 'On the Assessment of Completeness and Timeliness of Actionable Cyber Threat Intelligence Artefacts', in A. Dziech *et al.* (eds.) Multimedia Communications, Services and Security. MCSS 2020. Communications in Computer and Information Science, Volume 1284, Cham, Switzerland: Springer.

Yucel, C. *et al.* (2021) 'Data Sanitisation and Redaction for Cyber Threat Intelligence Sharing Platforms', 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, p.343-347.

Zetter, K. (2011) 'How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History', Wired, 7 November.

Zhang, C. Y. *et al.* (2022) 'Accessible from the open web: a qualitative analysis of the available open-source information involving cyber security and critical infrastructure', Journal of Cybersecurity, Volume 8, Number 1, p.1-15.