Repairing the Foundation: How Cyber Threat Information Sharing Can Live Up to its Promise and Implications for NATO

Michael Daniel
President & CEO
Cyber Threat Alliance

Joshua Kenway
Cybersecurity Associate
Cyber Threat Alliance

Abstract: Information sharing has become an overused term that provokes eye rolls within the cyber security community. Yet, effective sharing would improve cyber defences. Why has information sharing failed to live up to its promise? The difficulty stems from three faulty assumptions, namely that cyber threat information is primarily technical, that every organisation should produce and consume this technical data, and that sharing such information is easy. These faulty assumptions have resulted in ineffective policy, misaligned incentives, and insufficient information sharing. Instead, four alternative assumptions should drive sharing threat information consisting of multiple complex information types with values that vary across consumers. Relevance and comparative advantage should drive which organisations share what information, as information sharing is challenging and must overcome four barriers and trust is a necessary component of any sharing activity. These alternative assumptions have several implications. Few organisations should share more than three or four sub-types of cyber threat information. Information sharing programmes should focus on the types of information most valuable for their constituents and they need processes and rules that build trust over time. Reducing the number of organisations sharing technical information would make achieving scale and speed easier. The information sharing burden would decrease while the value would go up, increasing the probability of information sharing. Additional standard formats and sharing systems would emerge, with increasing degrees of automation. Finally, effective cyber threat information sharing requires planning, long-term investment, and sustained commitment. Information sharing is not an unsolvable problem. Changing the underlying assumptions will increase the volume, quality, and utility of cyber threat information sharing. In turn, more effective sharing will enable defenders to better understand adversaries in the context of their organisation, enabling them to develop mechanisms to disrupt adversary activities more strategically and raise the level of cyber security across the digital ecosystem. Only then can information sharing finally live up to its promise.

Keywords: *Information sharing, threat intelligence, cyber security*

1. INTRODUCTION

Information sharing has become such an overused but under-performing concept that the term tends to provoke eye rolls within the cyber security community. Yet, most practitioners and policymakers agree that better information sharing would improve defences against rapidly evolving cyber threats. Virtually every relevant panel, study, or review over the last 20 years has recommended increased information sharing as a key step in improving cyber security. The logical question is why information sharing has not increased. Its lack remains a barrier to better cyber security, whether within NATO or the broader digital ecosystem.

This chapter will identify three faulty assumptions that have prevented cyber threat information sharing from living up to its promise that cyber threat information consists primarily of technical data, that every organisation should consume this technical data, and that information sharing is easy. It then establishes a framework for updating the current approach to information sharing by distinguishing the characteristics and value of different threat information types, using relevance and comparative advantage as the basis for producing and consuming threat intelligence, addressing key barriers to information sharing, and identifying trust as a necessary component of effective information sharing. Finally, the chapter explores the implications of these changed assumptions for more effective information sharing, including within NATO's information sharing ecosystem.

A. Technical Level Cyber Threat Information Sharing in NATO

NATO adopted technical cyber threat information sharing early on through an instance of the open-source Malware Information Sharing Platform (MISP) (NATO, 2013; MISP, 2020a), which the Alliance leverages to privately share information with member states, industry partners, and national Computer Emergency Response Teams (CERT) (Schrooyen, 2017). NATO uses MISP for the exchange of classified technical information with tactical and operational value and information sharing with participating partners is filtered according to its classification level (Schrooyen, 2017). Using MISP only for classified technical information sharing limits its value because it restricts the number of potential partners and excludes other valuable types of strategic and operational information. Over-classification impedes information sharing, something which NATO has acknowledged (NATO, 2012).

NATO also maintains a best practice and threat information sharing relationship with EU-CERT (NATO, 2016) and is building an Industry Cyber Partnership (NICP) (NATO, 2020). These two programmes provide NATO with the foundation needed to meet the challenges of information sharing explored in this chapter. Key industry partners include Oracle (NATO, 2019a), RSA Security (NATO, 2017), FireEye (Fireye, 2016), Cisco (NATO, 2016), CY4GATE, Thales, Vodafone (NATO, 2018), BT, Minded Security, Lockheed-Martin, Fortinet, and Symantec (Schrooyen, 2017). The NICP has broad goals, including improvements to the sharing of best practices, expertise, experience, and information 'including [...] on threats and vulnerabilities' (NATO, 2020).

In parallel, the Alliance's efforts to operationalise a Cyber Security Collaboration Hub by 2023 (NATO, 2019b), which will allow member states 'to quickly and securely share information with each other, and with the [Alliance]' (NATO, 2019c), could address some of the challenges raised in this chapter. However, this chapter argues that NATO should shift its approach to information sharing to assume a leadership position in this area.

2. FAULTY ASSUMPTIONS: OVERPROMISING AND UNDERACHIEVING

Underlying the slow progress on information sharing are three faulty underlying assumptions: (1) cyber threat information consists primarily of technical data; (2) every organisation should be producing and consuming technical cyber information; and (3) sharing cyber threat information is easy.[1] These fallacies are implicit, rather than explicit, and so have largely avoided critical review or academic assessment. Further, they have resulted in counter-productive policy, misaligned incentives, and ineffective cyber security. To address these shortcomings, different foundational assumptions are needed. In turn, using better assumptions can make information sharing a more effective tool against cyber threats.

A. Cyber Threat Information Consists Primarily of Technical Data

Within the cyber security community, the term 'information sharing' primarily refers to the exchange of technical data that identifies malicious activity such as malware and malicious domain names. While several scholars (Friedman et al., 2015; Chismon & Ruks, 2015) acknowledge that such exchanges should also include other types of information, the emphasis is on technical data in practice. For example, the main use cases or core functionalities associated, respectively, with the two commonly used cyber information sharing standards, Structured Threat Intelligence eXchange (STIX) and the Malware Information Sharing Platform (MISP), focus on technical

[1] The cybersecurity field has long debated whether to distinguish between 'intelligence' and 'information'. While a distinction between intelligence and information may be important in some contexts, this chapter will set aside that argument and use the term 'information sharing' because it is understood by a broader audience. This approach is further legitimised by documentation from the MITRE Corporation describing its 'de-facto standard for describing threat intelligence' (Sauerwein et al., 2017: p. 838), specifically a white paper on 'Standardizing Cyber Threat Intelligence Information [emphasis added]' (MITRE, 2012).

information (MITRE, 2012; MISP, 2020b). Cyber threat information sharing 'primarily focus[es] on sharing of indicators of compromise' (Sauerwein et al., 2017: p. 838), leading to a situation in which the activities of almost every established sharing platform are 'comparable to data warehousing' (ibid: p. 849). Many US government programmes and existing statutes either explicitly or implicitly focus on this type of information sharing; meanwhile, companies are investing billions of dollars in an effort to consume and analyse technical cyber threat information (Verified Market Research, 2020).[2]

The assumption that cyber threat information is equivalent or primarily composed of technical data severely limits the potential value of information sharing. Technical data, while necessary, is not the only form of information that can provide value. For example, a warning from the US Federal Bureau of Investigation (FBI) that a specific Chinese cyber group is targeting a US company with cyber-enabled theft of intellectual property would be a useful piece of non-technical intelligence for that company. Written advisories about vulnerabilities and associated patches are critical to organisations using vulnerable software or hardware; in fact, such information is far more useful to most organisations than technical data on one of the many variations of the LockerGoGo malware. The most common interpretation of information is too narrow.

B. Every Organisation Should Produce and Consume Technical Data

If the underlying assumption is that information sharing means technical information, then it logically follows that most policies, infrastructure, and programmes for sharing are built around the idea that most organisations should produce and consume technical information. If everyone were to collect, share, and consume such data, the thinking goes, security would improve across the ecosystem. The problem with this logic is that most organisations are lousy at collecting, producing, and consuming technical data—and always will be. Most companies do not have the capability to identify a malware binary, analyse it, and use the resulting information, nor would they know how to handle a malicious domain name. As a practical matter, this situation will not change; no country will have enough cyber security professionals for every organisation to have this capacity. Small and medium businesses do not and will not have the resources to collect, process, share, and consume technical data regularly. This limitation does not mean such organisations would not benefit from cyber threat information sharing; rather they need different information.

Neither is this approach economically efficient. Most organisations do not need access to technical data in real-time. Despite the rapidly changing nature of cyber threats in a technical sense, for most organisations, cyber security requirements and best practices do not change much from day to day.

[2] For example, see the Cybersecurity Information Sharing Act of 2015 (Consolidated Appropriations Act of 2016, Division N, Cybersecurity Information Sharing Act of 2015) and the Automated Indicator Sharing Program (DHS Cybersecurity and Infrastructure Security Agency, 2020).

In addition, not every business has in-house technical accounting or legal skills—why should cyber security be different? Current practice does not sufficiently differentiate between organisations in terms of what information they should share under what circumstances and how frequently.

C. Information Sharing is Easy

In January 2008, the US government started the Comprehensive National Cybersecurity Initiative (CNCI), formalising it in National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 (The White House, 2010). 'Connect the Centers,' one of CNCI's twelve lines of effort, focused on information sharing with the goal of linking the US government's cyber centres into one common operating picture; over the long-term, it was intended to incorporate the private sector. Everyone assumed that this element would be the easiest to implement and the first to be completed. However, thirteen years later, this element is arguably one part of the CNCI vision that remains unrealised as the cyber security centres are not seamlessly connected and many silos remain stubbornly in place.

A similar situation has played out in the private sector with the creation of Information Sharing and Analysis Centers (ISACs). The assumption was that companies would eagerly join these organisations, share what they knew and consume the information shared by others. Yet, more than twenty years after the concept was formalised into national legislation, many sectors are just now forming an ISAC and, even in the most successful of them, the percentage of participants that actively share information is widely understood within the industry to remain low.

Public sector efforts to share information with the private sector have suffered analogous problems. The US government created the Automated Indicator Sharing (AIS) programme as a free service for general businesses, but few organisations have signed up and even fewer contribute to the programme (Marks, 2018). This is unsurprising if we look at what is being shared; a US government report from 2018 suggested that just two or three out of the 11,447 indicators submitted to AIS by the Department of Homeland Security were 'malicious and related to cyber incidents [... while] many of the indicators received were false positives or redundant information' (DHS Office of Inspector General, 2017: p. 15).

The three examples highlight that information sharing is difficult for a variety of reasons. Simply creating programmes and establishing sharing mechanisms is insufficient without addressing obstacles to sharing actionable information. These include underlying factors such as over-classification, reputational risk, and legal concerns, as well as operational hurdles around validation, standardisation, timeliness, and automation (Zibak & Simpson, 2019).

3. REBUILDING INFORMATION SHARING: NEW IMPERATIVES

These incorrect assumptions have undermined information sharing as an effective tool against cyber threats, yet policies, structures, and processes must be based on assumptions about the overall environment in order to function. As a replacement for the faulty assumptions explained above, this chapter proposes four alternative presumptions to enable effective information sharing. First, cyber threat information consists of multiple information types across different levels, with distinct value to different consumers, meaning that information sharing needs to be tailored and nuanced. Second, for this reason, relevance and comparative advantage should drive sharing activities. Third, effective information sharing efforts must overcome context-specific technical, economic, legal, and cultural barriers; and fourth, trust is a necessary component of information sharing. The rest of this section will explore these alternative presumptions in greater detail.

A. Types of Cyber Threat Information

Chismon and Ruks (2015) assembled a useful taxonomy of cyber information categories based on the kind of decisions the information informs. A modified version of their taxonomy is shown in Table I.

Table I: Categories of Cyber Threat Information

Category of Cyber Threat Information	Examples of Information Conveyed	Intended Audience	Decision Example	Timeframe of Use
Technical	Indicators of malicious activity (e.g., malware hashes or IP addresses)	Cyber security vendors and network provider	Should the network security tool allow this packet through?	Immediate
Tactical	Details related to a specific/ impending cyber attack	Network defenders (i.e. relevant staff and decision-makers)	Do we need to change a security setting today?	Short Term
Operational	Malware types; Attacker tactics, tools, and procedures (TTPs)	Senior-level security personnel / managers	How often should we patch our networks?	Medium Term
Strategic	High-level information on changing cyber risk	Executives / senior decision-makers	Should we change our risk calculation because a new adversary is targeting our industry?	Long Term

As detailed in Table I, different categories of information, from technical to strategic, are intended for different consumers. However, information across the four levels—technical, tactical, operational, and strategic—is interrelated. For example, technical and tactical information can be combined to generate operational cyber threat information to improve organisational understanding of an impending attacker's methods and capabilities (Chismon & Ruks, 2015). Similarly, post-incident analysis of technical cyber threat information often provides the foundation for the implementation of a tactical level decision. A holistic assessment of technical, tactical, and operational inputs drives the output of strategic cyber threat information. Despite these complex relationships, this taxonomy provides a useful way to think about cyber threat information and is indicative of why technical data-sharing should not be the sole focus of information sharing programmes. Smaller or less mature organisations are unlikely to find much utility in technical or tactical information sharing, while even larger organisations may miss out on key operational or strategic information insights if they focus exclusively on the technical information. For this reason, the Cyber Threat Alliance (CTA), which includes established cyber security vendors and related enterprises, shares a total of ten types of actionable cyber threat information across these four categories, as recalled by the authors and detailed in Table II.

Table II: Examples of Cyber Threat Information, by Category

Technical Level Information	Tactical Level Information	Operational Level Information	Strategic Level Information
Indicators and Sightings Hashes, binaries, IP addresses, URLs, etc.	**Targeted Warnings** Information that a malicious actor is targeting a specific organisation in the near term	**Vulnerabilities and Exploits** Descriptions of security flaws in software and how bad actors can exploit them	**Best Practices** Methods for organising, securing and maintaining IT networks to prevent, detect, respond and recover from cyber threats or incidents
Context Metainformation about technical indicators, including date and time detected, location of detection, type of organisation targeted, associated actor group	**Situational Awareness** Details of activity happening on a network and / or the broader internet at any given time	**Defensive Measures** Methods to mitigate exploits and counter adversary TTPs	**Strategic Warnings** General information about cyber threats, such as typical targets for an adversary and how they are evolving
Tactics, Techniques and Procedures Methods adversaries can use to carry out malicious activity		**Attribution** Identifying who is responsible for specific malicious activity	

Understanding the value of these various forms of cyber threat information requires taking a more mature and nuanced view than the simplistic assumption that more information sharing means better security. This expanded conceptual framework for cyber threat information sharing reflects the diversity of information that industry leaders already know must be shared to strengthen defences. Each type informs a different aspect of cyber security and has a different value in different situations. Broad adoption of this (still high-level) extension to the framework provided by Chismon and Ruks (2015) would enable cyber security practitioners to develop more nuanced and useful policies for information sharing.

B. Relevance and Comparative Advantage in Information Sharing

In other disciplines, from finance to health to politics to sports, organisations do not produce and consume the same information equally. Instead, wide variation occurs based on relevance to business models, missions, and perceived benefits. Cyber security practitioners and policymakers should expect cyber threat information sharing to behave similarly. Different organisations should produce and consume different types of information based on two principles: relevance and comparative advantage. These two concepts should drive who should be sharing what information with whom, in what detail, and at what periodicity.

1) Relevance of Information

Companies, non-profit organisations, and government agencies all have goals or missions and employ specific business models to achieve those goals. Information sharing should relate directly to an organisation's goals and business model. Thus, a cyber security vendor should share technical cyber threat information at speed and at scale continuously because it is directly relevant to their business model. Conversely, a medium-sized manufacturer primarily needs strategic and operational level cyber threat information—strategic warnings, best practices, and tactical warnings (e.g., if a government learns that the business or its industry is being targeted)—all of which need only to be updated when a change has occurred. Technical cyber threat information provided at scale to this business would simply not be useful.

2) Comparative Advantage of Information Sharing

Even if some organisations can produce certain information types, others might be more efficient at that work. For example, although governments can use their intelligence and law enforcement capabilities to collect, process, and produce technical cyber threat information, they do not have a comparative advantage in that information type. Private sector companies can perform that function just as efficiently. However, governments have a comparative advantage in other categories, such as attribution of cyber attacks, strategic warnings, and tactical warnings, which benefit from nation-state-level intelligence capabilities and authorities. As in other activities, the principle of comparative advantage should determine which organisations should be collecting, processing, sharing, and consuming different types of information.

C. Technical, Economic, Legal and Cultural Barriers

At first glance, the barriers inhibiting information sharing seem quite varied. However, a closer review shows they fall into four categories: technical, economic, legal, and cultural. While their specific manifestations and relative significance will vary across sharing contexts, these barriers can combine in various ways to create a formidable obstacle to sharing.

Technical barriers prevent information from moving rapidly at scale or in easily consumable formats. For example, inconsistent definitions and terminology and difficulty in achieving interoperability and automation remain significant obstacles (Zibak & Simpson, 2019). In turn, these barriers often inhibit the usability or reliability of shared information (ENISA, 2017).

Economic barriers stem from the inability to identify a clear return on investment from sharing activities. Organisations 'participate in sharing networks when their return is more than the cost to participate' (Vázquez et al., 2012: p. 432). This problem can be compounded by first-mover disadvantage, given that 'establishing threat intelligence sharing infrastructure is expensive ... [while] in the long run, intelligence sharing could help bring down the overall security cost' (Zibak & Simpson, 2019: p. 7). Absent a clear and immediate prospect of a return on investment, proponents often have difficulty making the business case to establish, invest in or sustain sharing activities. Legal barriers come from uncertainty about what information can be shared under what circumstances or unanswered questions about liability, fines, or prosecution. These uncertainties deter organisations from sharing. Privacy laws can hinder sharing by inadvertently classifying certain cyber threat information as private and thereby limiting how it can be used or distributed (Panda Security, 2018). These legal concerns require sharing organisations to undertake extensive consideration of their potential implications (Borden et al., 2018; Albakri et al., 2019).

Finally, cultural barriers can also impede sharing (Luiijf & Kernkamp, 2015). For cyber security companies, it can be hard to overcome the idea that retaining unique data yields a competitive advantage. For other organisations, it can be hard to overcome sentiments such as 'no one would target me', 'cyber security is too complex for executives and non-technical employees to understand', or 'falling victim to hackers is inevitable, so why bother?' For governments, long-standing views about the appropriate respective roles of the public and private sectors get in the way of cooperation and sharing.

The good news is that, over the last twenty years, practitioners have developed ways to overcome these barriers. The bad news is that none of these methods is frictionless or cost-free. For example, adopting technical standards for information sharing may require organisations to adjust business processes or infrastructure; high initial costs may need to be met with loans that are paid back by future sharing participants; legal consultations may be needed to shape sharing rules; and reluctant executives may need the benefits of information sharing to be explained in bottom-line terms.

Across the board, information sharing requires organisations to expend resources, either money or time. These costs can decrease but do not disappear. Yet, to be worthwhile, information sharing needs to be sustained and organisations have to pay a long-term, regular cost for engaging in information sharing activities. This requirement, in turn, means that information sharing requires incentives to achieve the scope, scale, and speed required for effective cyber defence. Such incentives can range from the individual (avoiding the costs of a cyber incident) to the public (government grants) to the avoidance of sticks (fines or penalties for not engaging in appropriate sharing). Regardless, information sharing laws, policies, programmes, and structures should assume that information sharing is resource-heavy and requires sustained investment to occur.

D. Trust as a Necessary Component of Information Sharing

Experience from previous initiatives and programmes demonstrates that information sharing only occurs when the providers and recipients have a degree of trust. As noted by Wagner et al. (2018), trust 'plays a critical role in sharing' (p. 5). The European Network Information Agency (ENISA) observes that in situations where trust between members of the community is diminishing or non-existent the value of information shared is undermined (ENISA, 2013). For information sharing to work, it is necessary to 'foster confidence for stakeholders that the provided information will be acted upon as intended' (Wagner et al., 2018: p. 5). Information providers have to understand who will receive their information, what they will do with it, and what level of information sharing-related risk to expect, while information recipients want to know where the information came from and its reliability.

To reach this level of confidence, information sharing organisations should 'provide control mechanisms to specify what information is shared, how much of it and with whom' (Sauerwein et al., 2017: p. 845). According to ENISA (2012, cited by Vázquez et al., 2012: p. 433), the use of intentionally carefully designed trust-building mechanisms, such as 'the policies, membership rules, requirement for security clearance and interaction type' can be beneficial in the context of information sharing and will support the creation of trust.

Absent trust, information sharing will not occur no matter what structures and incentives are put in place. Trust does not require that the participants all like each other, nor does it mean they share everything. Trust means that participants have a reasonable belief that all other participants will adhere to the agreed rules.

4. IMPLICATIONS OF INFORMATION SHARING IMPERATIVES

The new information sharing presumptions proposed in this chapter—careful consideration of information type and relevance, comparative advantage in information production, how to overcome existing context-specific barriers, and how to create and maintain trust—make the cyber threat information sharing landscape far more complex than most people envision. Yet, this very complexity provides an opportunity for simplification: rather than everyone trying to share everything all the time, organisations can concentrate on the information types most relevant to them. Information sharing architectures, policies, and systems should assist organisations in focusing their information sharing activities. Although identifying all the implications is beyond the scope of this chapter, some more prominent ones are worthy of mention.

Few organisations will share every type of cyber threat information. Most organisations should focus on the types of information most relevant to their business model. For example, under this paradigm, only organisations with strong technical capabilities would share technical cyber threat information: cyber security providers, telecommunications companies, Internet Service Providers (ISPs), Managed Security Service Providers (MSSPs), and large, multinational companies in critical industries. Government agencies would focus less on producing stand-alone technical indicators of compromise (IOCs), which industry has in abundance, and more on combining that information with strategic and tactical warning about specific threats, since their comparative advantage lies in their intelligence and law enforcement capabilities. Most citizens, businesses and organisations would primarily consume information about best practices and defensive measures.

The focus of information sharing programmes should change. Since most organisations do not need to produce or consume technical cyber threat information, government cyber security initiatives should reflect this. These programmes should instead encourage most organisations to hire a cyber security vendor or MSSP. Those service providers would consume the technical, contextual, vulnerability, and exploitation information and use it to make security adjustments such as updating blacklists or prioritising patches. Most organisations would primarily consume updates to best practice and strategic or tactical warnings. This change would make information sharing programmes more relevant and cost-effective.

Information sharing programmes need to build trust. Since trust is a key component for effective information sharing, programs, structures, and architectures need to build trust over time. Policies and structures should include operational processes designed to enhance confidence and trust when personal rapport among stakeholders may be lacking, particularly when programs are starting (see Sauerwein et al., 2017; Sillaber et al., 2016; Vázquez et al., 2012; Wagner et al., 2019). For example, CTA's information sharing rules specify the nature and scope of the sharing commitment, how members should handle shared information, and what enforcement mechanisms and penalties will be applied for violating those rules. Such clarity and consistency help new members trust that other members will treat their information properly.

Information sharing products can incorporate more than one information type. Since the different information types are interdependent, any given sharing product can contain more than one type. For example, CTA members share technical indicators and tactical context (and occasionally attribution) through the same automated system and standard format (Cyber Threat Alliance, 2020). A more rigorous conceptual framework for information sharing does not require a rigid division among the information types from a software or process flow perspective.

Reducing the number of organisations expected to share technical information would make achieving speed and scale easier. Abandoning the idea that all organisations everywhere should engage in technical cyber threat information sharing makes overcoming the barriers to technical sharing easier. Under this assumption, the number of organisations with the combination of willingness, relevance, and capability to engage in technical cyber threat sharing decreases to a large but manageable number (Aspen Cybersecurity Group, 2018). At this size, having most of these organisations participating in formal information sharing groups becomes a reasonable goal.

The information sharing burden would decrease while the value would go up, increasing the likelihood that organisations voluntarily participate in such activities. By focusing sharing activities on the most relevant information types, the time and monetary investment for most organisations would decrease. At the same time, the connection between shared information and the organisation's mission or business model would become clearer, thereby increasing its value and making that value easier to assess. The decreased burden and increased value would expand the number of organisations that participate in sharing activities.

Additional standard formats for non-technical information types would emerge, along with systems to share those formats with increasing degrees of automation. On the technical side, several standard formats now facilitate automated information sharing, such as the STIX (MITRE Corporation, 2012) and MITRE's Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) frameworks (MITRE Corporation, 2020). More rigorously dividing cyber threat information into different types would encourage other formats to emerge and organisations to adopt them. Standard formats make consumption of information easier for the recipient. Increased automation would increase speed and scale, making sharing more effective.

Effective cyber threat information sharing requires planning, long-term investment, and sustained commitment. For example, technical cyber threat information sharing is not merely a matter of adopting a technical standard and installing software. It takes engineering and analytic time on an ongoing basis as well as maintenance of the technology and processes. Similarly, consuming cyber security best practices is not a one-time endeavour; organisations must incorporate regular review and implementation into their business processes. Absent a long-term commitment from organisational leadership, sharing usually withers after an initial burst of enthusiasm. Cyber security should take on the same status as other business enablers, such as accounting, legal affairs, and communications; like these areas, cyber security should be a function that all organisations budget for and sustain over the long-term.

5. CONCLUSION

Cyber threat information sharing has bedevilled the cyber security community for at least two decades. Faulty assumptions have prevented this fundamentally sound concept from achieving its potential. But while information sharing is a tough problem, it is not an insoluble one. If the cyber security community adopts different underlying assumptions for information sharing then the volume, quality, and utility of the exchanged information can increase. In turn, more effective, relevant information sharing will enable defenders to better understand and anticipate adversaries, develop mechanisms to disrupt adversary activities more strategically, and raise the level of cyber security across the digital ecosystem. Under these circumstances, cyber threat information sharing can finally live up to its promise to enable better cyber security for everyone.

For NATO, updating programmes to reflect these revised information sharing assumptions would require significant changes to current operations. First, overcoming the technical, economic, legal, and cultural barriers to sharing relevant, actionable information across member countries and economic sectors will require sustained attention, prioritisation, and funding from NATO's senior leadership. Absent such attention, the barriers will likely prove insurmountable. Second, NATO should build on its existing MISP use to create a more comprehensive system of information sharing that broadens the types of information shared and widens the number of recipients. Third, NATO should consider how to better leverage industry for technical information, while enriching that information with government-derived information about context, attribution, and intent. If NATO shifted its approach to information sharing as suggested, the Alliance would have the opportunity to assume a leadership position in this area. If not, NATO will continue to struggle to make information sharing live up to its promise.

6. REFERENCES

Albakri, A., Boiten, E. and De Lemos, R. (2019) Sharing Cyber Threat Intelligence Under the General Data Protection Regulation. *Annual Privacy Forum 2019*, pp. 29-40.

Aspen Cybersecurity Group. (2018) An Operational Collaboration Framework for Cybersecurity. *The Aspen Institute*. Available from: https://www.aspen-institute.org/publications/an-operational-collaboration-framework/ [Accessed 23rd September 2020].

Borden, R.M., Mooney, J.A., Taylor, M. and Sharkey M. (2018) Threat Information Sharing and GDPR: A Lawful Activity that protects Personal Data. *White and Williams LLP, Osborne Clarke LLP and FS-ISAC*. Available from: https://

www.fsisac.com/hubfs/5442200/Resources/FS-ISAC_Threat_Information_Sharing_and_GDPR.pdf [Accessed 23rd September 2020].

Chismon, D. & Ruks, M. (2015) Threat Intelligence: Collecting, Analysing, Evaluating. *MWR Infosecurity & CERT-UK*. Available from: https://scadahacker.com/library/Documents/Best_Practices/CPNI%20-%20Threat%20Intelligence%20-%20Collecting%20Analysing%20Evaluating.pdf [Accessed October 29th 2020].

Cyber Threat Alliance. (2020) *What is the Cyber Threat Alliance?* Available from: https://www.cyberthreatalliance.org/resources/what-is-cta/ [Accessed 23rd September 2020].

DHS Cybersecurity and Infrastructure Security Agency. (2020) *Automated Indicator Sharing (AIS)*. Available from: https://www.cisa.gov/automated-indicator-sharing-ais/ [Accessed 23rd September 2020].

DHS Office of Inspector General. (2017) Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015. *US Department of Homeland Security.* OIG-18-10. Available from: https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-10-Nov17_0.pdf [Accessed 23rd September 2020].

ENISA. (2012) Cooperative Models for Effective Public Private Partnerships Desktop Research Report. *European Union Agency for Network and Information Security (ENISA).* Available from: https://www.enisa.europa.eu/publications/copy_of_desktop-reserach-on-public-private-partnerships/ [Accessed 23rd September 2020].

ENISA. (2013) Detect, SHARE, Protect: Solutions for Improving Threat Data Exchange among CERTs. *European Union Agency for Network and Information Security (ENISA)*. Available from: https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs/ [Accessed 23rd September 2020].

ENISA. (2017) Exploring the opportunities and limitations of current Threat Intelligence Platforms (Version 1.0). *European Union Agency for Network and Information Security (ENISA)*. Available from: https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms [Accessed 23rd September 2020].

Fireye. (2016) *NATO and FireEye Announce Cyber Information Sharing Agreement.* Available from: https://investors.fireeye.com/news-releases/news-release-details/nato-and-fireeye-announce-cyber-information-sharing-agreement/ [Accessed 23rd September 2020].

Friedman, J., Bouchard, M., Watters, J., Couch, J. and Hartley, M. (2015) Definitive GuideTM to Cyber Threat Intelligence. *iSight Partners & CyberEdge Group, LLC.* Available from: https://cyber-edge.com/wp-content/uploads/2016/08/Definitive-Guide-to-CTI.pdf

Luiijf, E. & Kernkamp, A. (2015) Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach. Den Haag.

Marks, J. (2018) The government's big idea to bolster the nation's collective cyber defense isn't attracting private-sector participants. *Nextgov*. Available from: https://www.nextgov.com/cybersecurity/2018/06/only-6-non-federal-groups-share-cyber-threat-info-homeland-security/149343/ [Accessed 23rd September 2020].

MISP. (2020a) *Software and Tools*. Available from: https://www.misp-project.org/tools/ [Accessed 23rd September 2020].

MISP. (2020b) MISP (Version 2.4, Readme. md). *GitHub*. Available from: https://github.com/MISP/MISP [Accessed 23rd September 2020].

MITRE Corporation. (2020) Adversarial Tactics, Techniques, and Common Knowledge (ATT&CKTM). Available from: https://attack.mitre.org/ [Accessed 23rd September 2020].

MITRE Corporation. (2012) *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™)*. Available from: https://www.mitre.org/sites/default/files/publications/stix.pdf [Accessed 23rd September 2020].

NATO. (2012) Information Sharing with Non-NATO Entities. *Joint Analysis & Lessons Learned Centre*. Available from: http://www.jallc.nato.int/products/docs/factsheet_info_sharing.pdf [Accessed 17th October 2020].

NATO. (2013) *Sharing malware information to defeat cyber attacks*. Available from: https://www.nato.int/cps/en/natolive/news_105485.htm [Accessed 23rd September 2020].

NATO. (2016) NATO expands cyber partnership with Industry. *NATO Communications and Information Agency*. Available from: https://www.ncia.nato.int/about-us/newsroom/nato-expands-cyber-partnership-with-industry.html [Accessed 23rd September 2020].

NATO. (2017) NATO welcomes RSA to its cyber coalition. *NATO Communications and Information Agency*. Available from: https://www.ncia.nato.int/about-us/newsroom/nato-welcomes-rsa-to-its-cyber-coalition.html [Accessed 23rd September 2020].

NATO. (2018) New NATO-Industry cyber partnerships signed at NITEC18. *NATO Communications and Information Agency*. Available from: https://www.ncia.nato.int/about-us/newsroom/new-natoindustry-cyber-partnerships-signed-at-nitec18.html [Accessed 23rd September 2020].

NATO. (2019a) NATO Agency, Oracle sign cyber information sharing agreement. *NATO Communications and Information Agency*. Available from: https://www.ncia.nato.int/about-us/newsroom/nato-agency--oracle-sign-cyber-information-sharing-agreement-.html [Accessed September 23rd 2020].

NATO. (2019b) *Factsheet: NATO Cyber Defence*. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf [Accessed 23rd September 2020].

NATO. (2019c) New NATO hub will gather the Alliance's cyber defenders. *NATO Communications and Information Agency*. Available from: https://www.ncia.nato.int/about-us/newsroom/new-nato-hub-will-gather-the-alliances-cyber-defenders.html/ [Accessed 23rd September 2020].

NATO. (2020) Our Objectives and Principles. *NATO Industry Cyber Partnership*. Available from: https://nicp.nato.int/objectives-and-principles/index.html [Accessed 23rd September 2020].

Panda Security. (2018) *What will happen with WHOIS when GDPR is implemented?* Available from: https://www.pandasecurity.com/mediacenter/security/whois-protocol-gdpr/ [Accessed 23rd September 2020].

Sauerwein, C., Sillaber, C., Mussmann, A. and Breu, R. (2017) Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives. In: Leimeister, J.M. and Brenner, W. (Eds.): *Proceedings of the 13th International Conference on Wirtschaftsinformatik, WI 2012, 12-15 February 2017, St. Gallen, Switzerland*, pp. 837-851.

Schrooyen, J. (2017) MISP Usage in NATO. *NATO Communications and Information*

Agency / NATO Computer Incident Response Capability. Available from: https://academiamilitar.pt/images/site_images/Eventos/3rd_Conference/Day_1/MISP_usage_in_NATO_-_Johan_Schrooven.pdf [Accessed 23rd September 2020].

Sillaber, C., Sauerwein, C., Mussmann, A. and Breu, R. (2016) Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice. In: *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, WISCS 2016, October 2016, Vienna, Austria.* New York, Association for Computing Machinery, pp. 65–70.

U.S. Congress. (2016) *Consolidated Appropriations Act of 2016, Division N, Cybersecurity Information Sharing Act of 2015*. Available from: https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf [Accessed 23rd September 2020].

Vázquez, D.F., Acosta, O.P, Spirito, C., Brown, S. and Reid, E. (2012) Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships. In: Czosseck, C., Ottis, R. and Ziolkowski K. (eds.) *2012 4th International Conference on Cyber Conflict, CYCON 2012, 5-8 June 2012, Tallinn, Estonia*. Tallinn, NATO CCD COE Publications, pp. 429-445.

Verified Market Research. (2020) Threat Intelligence Market by Deployment Model (Cloud-Based, On-Premise), by Component (Solution, Service), by Organization Size (SMEs, Large Enterprises), by Vertical, Geography and Forecast. Available from: https://www.verifiedmarketresearch.com/product/global-threat-intelligence-market-size-and-forecast-to-2025/

Wagner, T.D., Palomar, E., Mahbub, K. and Abdallah, A.E. (2018) A Novel Trust Taxonomy for Shared Cyber Threat Intelligence. *Security and Communication Networks*. 2018.

Wagner, T.D., Mahbub, K., Palomar, E. and Abdallah, A.E. (2019) Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*. 87 (November 2019). Cairo, Egypt, Hindawi.

The White House. (2010) *The Comprehensive National Cybersecurity Initiative*. Available from: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/national-initiative [Accessed 23rd September 2020].

Zibak, A. & Simpson, A. (2019) Cyber Threat Information Sharing: Perceived Benefits and Barriers. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019, August 26-29, 2019, Canterbury, United Kingdom. New York, ACM.