3

Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace

Deborah Housen-Couriel

1 INTRODUCTION: FRAMING THE RELATIONSHIP BETWEEN INFORMATION SHARING AND CYBER PEACE

The concept of cyber peace brings a much-needed, innovative perspective to discussions of the governance of cyberspace. The ambiguity, conflicting terminology, and lack of transparency with respect to activities by state and nonstate actors have characterized efforts to conceptualize and analyze this new area of human endeavor at least since John Perry Barlow's 1996 Declaration of the Independence of Cyberspace. Barlow's (1996) proclamation that claimed cyberspace as a home for the "civilization of the Mind" and a "global social space" that must be kept free of governments, state sovereignty, and legal constructs – in effect, exempt from any type of governance – marked early on in the life of online activities the challenges and tensions that remain today for the global collective action problem of cyberspace governance. Thus, the distinctive perspective of cyber peace has the potential to set our analytical sights anew and to provide a framework for moving ahead with the normative projects connected to the aspects of cyberspace governance, including the ongoing elucidation of binding rules of international and domestic law that are applicable to cyberspace activities of state and nonstate actors.

Building on previous chapters that treat the concept of cyber peace in depth, the following definition focuses on four specific elements:

> Cyber peace is […] not […] the absence of conflict […]. Rather it is the construction of a network of multilevel regimes that promote global, just and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike to help reduce the threats of cyber conflict, crime and espionage to levels comparable to other business and national security risks. To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to build robust, secure systems and couches cybersecurity within the larger debate on internet governance (Shackelford, 2014, pp. xxv–xxvi).

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

The four elements emphasized in the above definition describe the fundamental connection between the goals of cyber peace and information sharing (IS), the subject of this chapter (Johnson et al., 2016, p. iii).[1] Clarification of "rules of the road," whether these are binding or voluntary; threat reduction, risk assessment, and best practices for carrying out these three tasks are precisely the substantive contribution that IS makes to the cybersecurity postures and strategies of stakeholders participating in any given IS platform. As detailed herein, such a platform optimally defines threshold norms of permissible and nonpermissible online behavior on the part of all actors, establishing the criteria for determining whether an individual, private organization, country, group of hackers, or even another autonomously acting computer has violated a rule (Deljoo et al., 2018, p. 1508). It also reduces vulnerability to cyber threats by lessening the informational asymmetries that characterize hostile cyber activities to the advantage of the attacker, and contributes to organizational risk assessment by integrating the information shared by other participants in the IS community into heightened "cyber situational awareness" for all sharers. Fourth, IS is readily framed and understood by a multiplicity of actors at the domestic level – private, governmental, and individual – as a *best practice* and, at the international level, as a *confidence-building measure* (CBM) for building trust among state and nonstate actors.[2] These two characterizations of IS in the domestic and international jurisdictional arenas, respectively, are evidenced by the inclusion of IS modalities in many instances of national law and policy, as well as tens of multilateral and bilateral instruments for governing cyberspace at the international level (Housen-Couriel, 2017, pp. 46–84). Five examples of the latter are the 2015 Shanghai Cooperation Organization's International Code of Conduct for Information Security, the UN GGE Report of July 2015, the OSCE's Confidence-Building Measures for Cyberspace of 2016, the EU's Network and Information Security Directive that entered into force in August 2016; and the 2018 Paris Call for Trust and Security in Cyberspace.

When IS implemented as a voluntary or recommended best practice or CBM in the context of these regulatory arrangements – rather than as a mandated regulatory requirement – it has the advantage of bypassing the legal challenges of achieving formal and substantive multistakeholder agreement on cyber norms. The difficulties

[1] The 2016 NIST Guide to Cyber Threat Information Sharing has noted the advantages of IS measures as a means of leveraging the collective knowledge, experience, and capabilities of both state and nonstate actors within the sharing community in order to enhance the capability of each to make informed decisions regarding development of policies, defensive capabilities, threat detection techniques, and mitigation strategies.

[2] On information sharing as an enabler of trust building to resolve collective action problems see, for example, Ostrom et al. (1990) ("By voluntarily sharing the costs of providing information – a public good – participants learned that it was possible to accomplish some joint objectives by voluntary, cooperative action."); and Ostrom et al. (2012), pp. 23, 79, 81–82, 88, and 93 (where IS constitutes an element of the Socio-Ecological System, or SES concept used by Elinor Ostrom to analyze ecosystems addressing a collective action problem).

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

of such normative barriers are often observed as characteristic of the contemporary cyber lay of the land. Either as a best practice (at the domestic level) or a CBM at the international level, IS has the advantage of bypassing the present challenges of achieving formal and substantive multistakeholder agreement on cyber norms that are inherent elements of national and multilateral legal regimes for the governance of cyberspace (Macak, 2016; Ruhl et al., 2020).

We propose in this chapter that, as IS platforms provide increasingly relevant, timely, and actionable data on vulnerabilities, including zero-day vulnerabilities (Ablon & Bogart, 2017); adversaries' tactics, techniques, and procedures; malware tool configurations; and other tactical and strategic threat indicators, stakeholders will become more incentivized to increasingly trust IS platforms and to utilize them for both real-time response to hostile cyber activities and for building long-term cybersecurity strategies. Technological advances are easing this process, as platforms adopt new techniques for the automation of alerts and communications among sharers (Wagner et al., 2019). Thus, in instances when sharing communities are substantively and technologically optimized for cybersecurity, participants benefit from expertise and insights which may otherwise be unavailable to them with respect to developing threat vectors, mitigation of specific cyber risks, and real-time coordinated responses to hostile cyber events.

Nevertheless, together with this chapter's assertion that the use of IS constitutes a best practice and a CBM, IS for the mitigation of cyber risk has also been critiqued for drawbacks and disincentives that have caused the current situation of less than optimal utilization of IS platforms. Some of these challenges – posed to stakeholders that refrain from joining IS platforms, and to IS participants who underuse platforms, or use them as free riders – are reviewed in Section 3. Two of the underlying assumptions of the chapter address this challenge of effective incentivization of stakeholders' use of IS platforms.

The first assumption is that the continued honing of the technological aspects of IS will make platforms more relevant for shareholders: Sharers will increasingly be able to rely upon robust, user-friendly, flexible, and confidential platforms that meet their needs for boosting cybersecurity, especially for coping with real-time cyber events that are in the process of compromising their systems and data. The ongoing relevance and effectiveness of a given IS platform will thus depend upon its incorporation of technology-based best practices for IS, including, *inter alia*, automated threat identification and sharing, vetting of information reliability, and interoperability with other IS platforms.

The second assumption relates to the value of polycentric governance in cyberspace (Craig & Shackelford, 2015). Although no panacea,[3] the sharing of cyber threat information is optimized for platform participants when it engages a plurality and diversity

[3] See below for critique of polycentric governance models in the cybersecurity context in particular; cf. McGinnis (2016).

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

of actors: governments, private corporations, NGOs, academia, informal groups, epistemic communities, individuals, and even autonomous or semiautonomous computer systems.[4] Also, optimal IS will include a plurality and diversity of methodologies and measures: real-time information on hostile cyber events, including digital forensics shared by analysts; data on the cyber strategies and policies of private sector organizations, of economic sectors, and of countries; and technical specifications such as those referred to above, evaluations of developing threat vectors, and cyber awareness and training materials. Some of these types of information constitute protected data, the sharing of which impacts substantive legal rights, such as individuals' rights to personal data privacy, corporate intellectual property, and antitrust guarantees (Chabrow, 2015; Elkin-Koren, 1998; Harkins, 2016, pp. 49–63; Shu-yun & Nen-hua, 2007). Analysis of the regulatory protections provided for safeguarding these rights in the context of IS exceeds the scope of the present chapter, and will be treated elsewhere. Support for the position that a polycentric governance model is also advantageous for oversight of such rights protections (Shackelford, 2016) will be expanded upon below.

Thus, to summarize the points raised in this introductory section, we propose in this chapter to show that, to the extent that IS through trusted platforms incorporates modes of polycentric governance, leveraging a multilevel and multisectoral diversity of actors, methodologies, and measures, cybersecurity is supported and the aims of cyber peace are advanced.

In conclusion, an often observed but challenging aspect of cybersecurity and cyber peace in general should also be highlighted in the present IS context: IS is an ongoing exercise in trust building among sharers (Ostrom, Chang, Pennington & Tarko, 1990; Ostrom et al., 2012). Platform participants must be able to rely upon the security of all communications channels, they must have confidence that the data shared will be utilized only in accordance with agreed rules by all participants, and they must have certainty that any stored or retained data are completely protected and that they remain confidential. By leveraging technological developments and modes of polycentric governance, IS has the potential to embody Alexander Klimburg's (2018, p. 359) observation that "trust is a tangible resource in cyberspace," hard coded into its basic protocols, into the development of the Internet and, we venture to add – into secure platforms for the sharing of critical information.

The chapter is structured as follows. Section 2 describes the "how" of IS measures by reviewing selected operational aspects of two examples of IS platforms: one a domestic platform and the second a multilateral one for the global financial sector. Section 3 discusses the ways in which IS mitigates cyber vulnerabilities, and includes some critique of the present utilization of IS. Section 4 characterizes

[4] Such cross-sector cooperation for cybersecurity is becoming increasingly transparent. See, for instance, U.S. Department of Justice (September 16, 2020), and the diversity of participants in the EU's Cyber and Information Domain Coordination Center (https://pesco.europa.eu/project/cyber-and-information-domain-coordination-center-cidcc/).

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

the relationship between cyber peace and IS, arguing that IS constitutes a critical building block of sustainable cyber peace governance because of present challenges to binding normative regimes internationally and domestically. Section 5 summarizes the main points and proposes areas for further research that have ramifications for cyber peace IS, including the exploration of IS models with respect to other global collective action problems, such as global health, ensuring global environmental quality, and the elimination of debris in outer space.

2 HOW INFORMATION SHARING WORKS: SELECTED OPERATIONAL ASPECTS OF IS PLATFORMS FOR "BEST PRACTICE" MITIGATION OF CYBER RISK

This section will describe the practical implementation of IS measures by first defining the concept of IS in the cybersecurity context, then noting the key characteristics of IS platforms, before examining two examples of governmental and private sector exchange of cyber information, one domestic in scope (the US' Cyber Information Sharing and Collaboration Program [CISCP]); and the other international and sectoral (Global Financial Services Information Sharing and Analysis Center [FS-ISAC]). The concluding section addresses the operationalization of IS as a standardized best practice for bolstering cybersecurity.

2.1 *Defining Information Sharing*

Information sharing is a measure for interorganizational, intersectoral, and intergovernmental exchange of data that is deemed by sharers to be relevant to the resolution of a collective action problem (Skopik, Settanni, & Fiedler, 2016). In the cyber peace context, it is the agreed upon exchange of an array of cybersecurity related information, such as vulnerabilities, risks, threats, and internal security issues ("tactical IS"), as well as best practices, standards, intelligence, incident response planning, and business continuity arrangements ("strategic IS") (International Standards Organization, 2015). The primary aim of IS in all of these contexts is to reduce information symmetries regarding cyber vulnerabilities at two levels: between hostile cyber actors and their targets and between targeted organizations themselves, none of which has complete situational awareness of the threat environment on their own.[5]

The 2016 *Guide to Cyber Threat Information Sharing*, published by the US National Institute of Standards and Technology (NIST), describes the advantages of IS measures for improving cybersecurity[6] as follows:

[5] Of course, hostile cyber actors also engage in IS, an interesting issue beyond the present scope. See Hausken (2015).

[6] "Cybersecurity" describes the process of applying a "range of actions for the prevention, mitigation, investigation and handling of cyber threats and incidents, and for the reduction of their effects and of the damage caused by them prior, during and after their occurrence." Israeli Government (2015, February 15).

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

> By exchanging cyber threat information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face. Using this knowledge, an organization can make threat-informed decisions regarding defensive capabilities, threat detection techniques, and mitigation strategies. By correlating and analyzing cyber threat information from multiple sources, an organization can also enrich existing information and make it more actionable (Johnson et al., 2016, p. iii).

These advantages are gained through the resolution of several key issues which arise in defining the four modalities of IS for any given IS platform:

- The agreed rules for thresholds of shared threats and events – IS depends upon the prior agreement among participants as to the threshold events which will trigger the need to share information, especially for the real-time sharing of vulnerabilities and hostile cyber events requiring specific defensive actions such as patching vulnerabilities (ideally within an agreed on window of time). This threshold determination is both substantive and technical: It is set in accordance with legal and regulatory requirements of the given jurisdiction, whether domestic or international, and it is triggered by technical indicators based incident response protocols protecting the network.
- Regulatory issues – Substantive normative and regulatory frameworks constitute an ever-present backdrop for the technological modalities of IS and the determination of IS thresholds. The role of such frameworks in IS, especially the relationship between them and the agreed technical rules for information sharing is critical. They include the aforementioned rights protections (personal data privacy protections, corporate Internet protocol (IP) safeguards, and antitrust guarantees), general international law constraints on hostile cyber activities (Schmitt, 2017), and bilateral and multilateral treaty provisions (Convention on Cybercrime, 2001). Treatment of these substantive issues are beyond the scope of the present chapter and are noted in the Conclusion for further research.
- The types of information shared – Each IS platform specifies the typologies of relevant information to be shared by participants, often in a Terms of Use document that is restricted to the participants – an internal code of conduct that may serve to build trust among sharing entities. Legal and regulatory constraints also determine types of information that may be shared, and the conditions for sharing, such as anonymization of protected personal data. One example is the Cybersecurity Information Sharing Act (2015), S. 754, 114th Cong. (2016), which defines in Section 104(c)(1) two types of shareable information that must be restricted to a "cybersecurity purpose": "cyber threat indicators" and "defensive measures." As discussed below, current developments are moving toward standardization of relevant threat indicators, IS automatization, and rapidity, toward a commoditization of cyber threat data within communities of trust.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

- The sharing entities – Since effective IS platforms are based on communities of trusted sharers, the identity of the sharing entities should be explicit and transparent to all participants (Gill & Thompson, 2016; Lin, Hung, & Chen, 2009; Özalp, Zheng, & Ren, 2014). Moving from the local to the global, sharing of cybersecurity relevant data may take place among individuals (i.e., the MISP and Analyst1 platforms for cyber analysts); within a corporate sector (i.e., the Financial Sector Information and Sharing Analysis Center (FS-ISAC) and Israel's Cyber and Finance Continuity Center (FC3)); between private sector entities and governmental agencies (as in the UK's Cyber Security Information Sharing Partnership [CiSP] and the US' CISCP example below); between one country's governmental agencies (i.e., the US federal government's Cyber Threat Intelligence Integration Center); between states, either bilaterally and multilaterally (i.e., the European Union's CSIRT network as mandated in the Network and Information Systems Directive); and in the framework of international organizations (i.e., NATO's Computer Incident Response Capability).[7]

Moreover, if the definitional scope of IS broadens to include notifications of irregular activity in cyberspace, then sharers also include individual members of the public who may share reports of suspected cyber fraud and cybercrime with entities such as the FBI and national authorities within the EU, via dedicated websites such as the FBI's Internet Crime Complaint Center and the national sites listed on the platform of Europol's Cybercrime Center, "Report Cybercrime Online" (FBI, 2020; Europol, 2020).

The above sampling of sharing entities illustrates the criticality of a polycentric approach to the governance of cyberspace that includes a diversity of actors to address a collective problem. Beyond the modes of IS to bolster cybersecurity among governmental and private companies and organizations reviewed in this Part, current trends in the development of IS include intrasectoral sharing of cyber threat data, integration of artificial intelligence capabilities to improve IS, participation of expert individuals in IS platforms, and the inclusion of the wider public for the purpose of reporting suspicious activity that may constitute a cybercrime, or an indication of a new cyber threat on financial and consumer platforms.

We exclude from the present discussion IS between civilian entities and military or other covert state operators, due to the lack of transparency of most such arrangements (Robinson & Disley, 2010, p. 9). While there are some examples of military actors sharing cyber threat data publicly, as in the US Cyber Command's utilization of the VirusTotal platform in September 2019 to share malware samples associated

[7] There are also open-source sharing communities that make threat indicators publicly available, such as Citizen Lab Reports, (n.d.) and analyst reports that are openly shared online. Such public platforms are definitionally distinct from IS, which relies upon the existence of a closed, trusted community for its effectiveness.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

with the North Korean Lazarus Group, such sharing is neither consistent nor transparent, and thus difficult to analyze conclusively (Vavra, 2019). Should such a trend emerge toward IS by military and intelligence stakeholders with the public, in order to help strengthen common cybersecurity postures, it will be an interesting development that would further support the argument in favor of the polycentricity of IS.

In concluding this initial definitional and conceptual discussion of IS, we note that IS must develop in concert with the changing cyber threat landscape in order to retain its relevance and credibility for participants. These developments dovetail with the approach that cyber peace is a dynamic situation, not a static one, and that it also will take into account changing aspects of cyberspace activities.

In the following two sections, we briefly examine two examples of governmental and private sector exchange of cyber information, each incorporating a different model of IS. The first example, the US' CISCP, constitutes a national platform with both governmental and private sector sharers. The second example, the FS-ISAC, is global in scope[8]; yet, it has been established by private organizations in the financial sector as a not-for-profit entity. Additional platforms, and some of their characteristics, are noted following these two, as well as a brief summary of commonalities and differences.

2.2 *The DHS Cyber Information Sharing and Collaboration Program*

The US Department of Homeland Security and Department of Justice provides a dedicated platform for IS between governmental and private sector organizations, the CISCP. Originally established as a platform for the benefit of critical infrastructure operators pursuant to Presidential Decision Directive-63 of May 1998 (as updated in 2003 by Homeland Security Presidential Decision Directive 7), the CISCP is a generic, voluntary, free-of-charge IS platform, open to public and private sector organizations. By incorporating operators of critical infrastructures and other private and governmental organizations into one platform, CISCP aims "to build cybersecurity resiliency and to harden the defenses of the United States and its strategic partners" (CISCP, www.cisa.gov/ciscp). Thus, it is an explicitly domestic IS platform, operating under US legal and regulatory constraints. Prospective participants sign an agreement establishing the modalities of the exchange of anonymized cybersecurity information, thus ensuring protection from legal liability that may ensue from the sharing of protected information such as personal data, information subject to sunshine laws, and some proprietary data. The platform is described as follows:

> [CISCP] enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure … sectors. CISCP fosters this collaboration by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused operational context … [it] helps partners

[8] FS-ISAC headquarters are located in the USA, with offices in the UK and Singapore.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

> manage cybersecurity risks and enhances our collective ability to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents (Cyber Information Sharing and Collaboration Program, www.cisa.gov/ciscp).

Upon completion of an onboarding training session, participating organizations are provided with of two types of CISCP data, reflecting the abovementioned distinction between strategic and tactical IS. The first is ongoing cyber threat information that is made available to participants through indicator bulletins, analysis reports, and malware reports. Two examples are the Weekly Bulletin, summarizing new vulnerabilities according to NIST's National Vulnerability Database classification system (U.S. Department of Homeland Security, 2020) and Joint Alerts, such as that issued in early April 2020 on the exploitation of COVID-19 by malicious cyber actors (Cybersecurity and Infrastructure Agency, 2020b).

The second type of IS provided by CISCP is real-time information about emerging hostile cyber events, characterized by actionable data such as technical indicators of compromise and measures to be taken for resolving them (software updates and patches, file hashes, and forensic timelines). One example is the January 2020 alert regarding serious vulnerabilities in Microsoft Windows operating systems, designated CVE 2020-0601 (also, less officially, "Curveball" and "Chain of Fools") (Wisniewski, 2020). The alert warned of a spoofing vulnerability in the way that Windows validates a certain type of encrypted certificate. A hostile actor could exploit this vulnerability through a man-in-the-middle attack, or by using a phishing website (such as an individual user's bank website) to obtain sensitive financial data or to install malware on a targeted system.

The CISCP shared two types of tactical cybersecurity information with platform participants: A Microsoft Security Advisory addressing the vulnerability by ensuring that the relevant encrypted certificates were completely validated and a National Security Agency advisory providing detection measures for targeted organizations (Cybersecurity and Infrastructure Agency, 2020a). As a result, the Windows vulnerability was quickly identified and addressed by targeted actors. Analysts have noted that IS was especially effective in this incident, resolving a "dangerous zero-day vulnerability" because of the proactive disclosure made by the NSA to Microsoft, and then allowing the vulnerability and patch to be rapidly and simultaneously shared at "machine speed" through the CISCP's automated indicator sharing capability (Wisniewski, 2020). The CVE 2020-0601 event thus exemplifies the importance of leveraging IS among a diversity of sharers – here, governmental and private sector actors – in a transparent manner (Schneier, 2020).

2.3 *Financial Services Information and Analysis Center (FS-ISAC)*

The second IS platform for analysis is FS-ISAC. Like CISCP, it was established pursuant to Presidential Decision Directive-63; yet, the scope of its activity differs from the CISCP in three important respects: It is restricted to the regulated financial

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

sector; it is explicitly global in its membership and scope; and it requires a fee for participation. Thus, it provides a different model for IS from that of the CISCP and focuses on the sector-specific threat vectors and risks of the vulnerable and frequently targeted global financial sector (World Economic Forum, 2019).

FS-ISAC is the leading global IS platform for this sector, which includes 7,000 members in over 70 jurisdictions. It is constituted as a nonprofit organization with headquarters located in the USA and regional hubs in the UK and Singapore. Member institutions are regulated private-sector financial entities (with some exceptions) and include banks, brokerage and securities firms, credit unions, insurance companies, investment firms, payment processors, and financial trade associations. A separate subplatform was established in July 2018 under the auspices of FS-ISAC for governmental and regulatory entities (Cision, 2018): This CERES platform (CEntral banks, REgulators and Supervisory entities) utilizes separate Operating Rules (www.fsisac.com/fsisac-ceres-operating-rules) and Subscriber Agreements (www.fsisac.com/ceres-forum-subscriber-agreement) for its members.

The FS-ISAC platform focuses on intrasectoral IS: The sharing of government sourced information is independently vetted by the platform's Analysis Team as it is shared *via* the DHS' National Cybersecurity and Communications Integration Center, which provides US federal government cyber advisories. The primary objective is to share "relevant and actionable" information among sectoral participants on an ongoing basis "to ensure the continued public confidence in global financial services" (FS-IAC, www.fsisac.com/). The motivation for members to utilize the FS-ISAC platform includes "[its] access to … best-available information, … trusted consultation with other experts in interpreting the information, the classified working environment" (He, Devine, & Zhuang, 2018, p. 217), and the opportunity to access all of this on a single, sector-specific dedicated platform. Shared data include sector-specific threat alerts and indicators, intelligence briefings, tabletop exercises, and mitigation strategies. Participants are eligible to participate in seven separate levels of IS, in accordance with graded membership fee levels, which can amount to tens of thousands of dollars annually (Weiss, 2015, pp. 9–10). To increase its global reach and promote cybersecurity within the financial sector, FS-ISAC also provides a no cost, unidirectional crisis alert service for financial institutions which do not opt for paid membership. The FS-ISAC Operating Rules, Subscriber Terms and Conditions, and End User License Agreement are all available to the public on its website, but those organizations accepted for membership are required to sign an additional, and transparent Subscriber Agreement that is forwarded only following an internal authentication process.

The platform itself is operated by a private sector service provider and overseen by a member constituted board. Information may be attributed or shared anonymously by encrypted web-based connections, and alerts are distributed by the FS-ISAC Analysis Team in accordance with one of the five service levels to which the member has subscribed. Members are notified of urgent and crisis situations via the type

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

of communication they designate (electronic paging, email, Crisis Conference call), and are required by the Subscriber Agreement to access the FS-ISAC portal to retrieve relevant information. Due to the highly regulated nature of the financial sector and the high confidentiality of the information it processes, members are explicitly permitted to submit information anonymously. In addition, all data that have not been specifically designated as attributable to the sharer is subject to a two-step process to scrub all references to the submitting company, one automated via process of keyword search and the second a review by the Analysis Team. Incoming information collected by FS-ISAC from members is shared with government and law enforcement agencies only with consent of the sharing member. Concerns around sharing of sector-specific information are governed by an explicit ban on the exchange of commercial information by antitrust and competition provisions in the Rules and the Subscriber Agreement, and by the applicability of all relevant laws and regulations in member countries (FS-ISAC Operating Rules, art. 9). Likewise, members are bound by a confidentiality agreement and requirements with respect to any sharing of protected personal data (FS-ISAC Operating Rules, arts. 11 & 12).

FS-ISAC maintains an all sector, global cybersecurity alert level, the Financial Services Sector Cyber Threat Advisory, and uses the standardized Traffic Light Protocol (TLP) that is also employed by CISCP, as further described below. Recent research shows that FS-ISAC's use of automated peer-to-peer alerts has decreased the time for generation of cybersecurity compromise indicators by IS participants "from nearly six hours to one minute" (Wendt, 2019a, p. 109), and that "… the automated receipt, enrichment, and triage of [indicators] by the financial institutions were reduced from an average of four hours to three minutes. In total, the automation reduced the average time to produce an IOC, disseminate an IOC, and initiate a response from approximately 10 hours to 4 minutes" (Wendt, 2019b, p. 27).

At present, financial sector entities "actively participate" in peer-to-peer platforms such as FS-ISAC (Wendt, 2019a, p. 115), leveraging automated IS to boost organizational and sectoral cybersecurity. Yet, FS-ISAC and similar sectoral ISACs have come under criticism for the less than optimal participation of members in the platform. Reasons include the platform's reliance on voluntary sharing by members – and thus, the ease with which an institution can act as a "free rider"; the potentially negative impact of sharing of vulnerabilities and risks on commercial reputation and profitability within the sector; and concerns of substantive legal exposures with respect to protected personal data, corporate IP, and antitrust concerns (Liu, Zafar, & Au, 2014, p. 1). The perception of vulnerability given by participation in an IS platform may be an additional factor (Wagner et al., 2019, at 2.6). Thus, on the one hand, the use of FS-ISAC as a platform for sharing among financial sector participants may be readily adopted, especially given the cost-free option made available for receiving urgent governmental alerts. One the other hand, the incentivization of IS on the part of private sector members is much more challenging. We address this concern in Section 4.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

2.4 *Operationalizing IS as a Standardized Best Practice for Cybersecurity*

Information sharing on cyber threats and vulnerabilities of all types that passes through the CISCP, FS-ISAC, and other IS platforms requires technological measures to safeguard IS at three levels: (1) The rapid provision of data by the sharing organization; (2) its confidential transmission; and (3) its timely processing, distribution, and storage on the IS platform. As we have seen in the above examples, IS platforms leverage standardized, automated formats that enable rapid dissemination and reception of cyber threat indicators (CISA Incident Reporting System, www.us-cert.gov/forms/report; US-CERT DHS Cyber Threat Indicator and Defensive Measure Submission System, www.us-cert.gov/forms/share-indicators). Well-known examples are the STIX and TAXII indicator formats[9] that also enable automated information sharing (AIS), Automated Indicator Sharing (AIS), www.us-cert.gov/ais, and the standard TLP, which classifies the security levels of the shared data using four colors in order to indicate the rules for sharing perimeters (see Figure 3.1).[10]

There are many examples of national and transnational IS platforms utilizing similar, standardized systems for threat indicator transmission, including NATO (Oudkerk & Wrona, 2013); the EU's CSIRT network established under the EU NIS Directive (Directive 2016/1148)[11]; the Cyber Threat Alliance (Fortinet, 2017); Israel's "Showcase" (*Chalon Raávah*) (Israel Cyber Directorate, 2019) and its FC3 (Housen-Couriel, 2018; Housen-Couriel, 2019; Ministry of Finance and the Cyber Directorate, 2017); the CiSP of the UK National Cyber Security Center (National Cyber Security Centre, n.d.); and the "Informationspool" platform supported by Germany's Department for Information Sharing (Bundesamt für Sicherheit in der Informationstechnik, BSI) through its "cyber alliance" (Allianz für Cyber-Sicherheit) (Alliance for Cyber Security, n.d.).

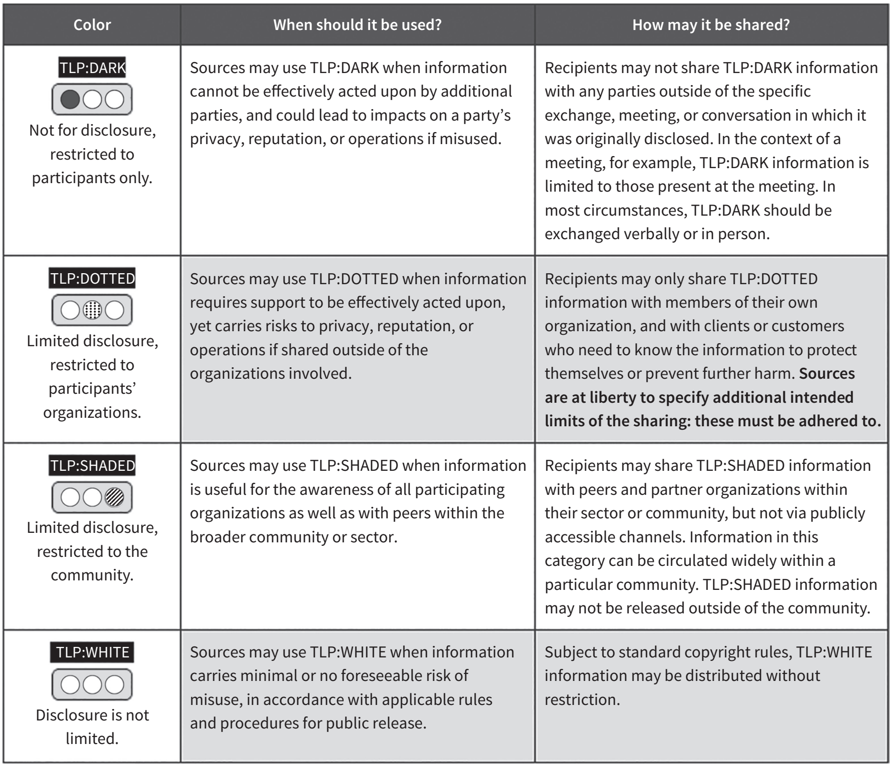
In addition to these IS platforms that foster IS among governmental, corporate, and some other institutional actors for a broad range of cyber threats and risks, several specialized IS platforms focus on a narrower risk typology that pinpoints cybercrime and terrorist activity on the Internet. Examples include INTERPOL's Cybercrime and Cyber-terrorism Fusion Centres (INTERPOL, n.d.); EUROPOL's European Cybercrime Centre (which has been effective in botnet takedown and in the protection of children online) (Europol, n.d.); and the Hash Sharing Consortium established in the framework of the Global Internet Forum to Counter

[9] "STIX is a language … for the specification, capture, characterization and communication of standardized cyber threat information. It does so in a structured fashion to support more effective cyber threat management processes and application of automation." Barnum (2014). See also Van Impe (2015, March 26).

[10] Additional standards are MITRE's Malware Attribute Enumeration and Characterization (MAEC) and OpenIOC, developed by Mandiant (Mavroedis & Bromander, 2017).

[11] The relevant NIS Annex, entitled "Requirements and Tasks of CSIRTs," stipulates their monitoring of risks and incidents; the provision of alerts and other operative indicators; and support for incident response.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press



Color	When should it be used?	How may it be shared?
TLP:DARK ●○○ Not for disclosure, restricted to participants only.	Sources may use TLP:DARK when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:DARK information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:DARK information is limited to those present at the meeting. In most circumstances, TLP:DARK should be exchanged verbally or in person.
TLP:DOTTED ○▦○ Limited disclosure, restricted to participants' organizations.	Sources may use TLP:DOTTED when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:DOTTED information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:SHADED ○○▨ Limited disclosure, restricted to the community.	Sources may use TLP:SHADED when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:SHADED information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:SHADED information may not be released outside of the community.
TLP:WHITE ○○○ Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

FIGURE 3.1 Traffic Light Protocol (TLP) definitions and usage, CISA [no date].

Terrorism (GIFCT) founded in 2016 by Facebook, Google, YouTube, and Twitter to share information on extremist and terrorist content online and containing more than 200,000 such hashes (Global Internet Forum to Counter Terrorism, n.d.).

These and other such IS platforms reflect organizational and regional differences in the modes of gathering and processing cyber threat indicators and other operational data. Yet, they all rely on standardized and vetted processes that promote trust among sharing entities (International Standards Organization, 2015). The developing technical protocols and the informal codes of conduct around their use constitute an important aspect of IS as a best practice for cybersecurity, and contribute to incentivizing it for use by a plurality of sharers.

3 MITIGATION OF CYBER THREATS AND EVENTS THROUGH INFORMATION SHARING: DISCUSSION

Although neither the sole means of closing gaps in cybersecurity, nor by any means a blanket remedy, IS already serves as a key measure for bolstering national, sectoral and, ultimately, global cybersecurity by leveraging and optimizing

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

interdependencies (Europol, 2017). Nevertheless, there is still critique of its present use as a measure for boosting cybersecurity and mitigating risk.[12] Melissa Hathaway (2010) has noted that the considerable quantity of available IS platforms poses a challenge for limited organizational and governmental resources, causing confusion and under commitment (counting fifty-five such government initiated partnerships in the USA alone). Zheng and Lewis (2015, p. 2) emphasize “programmatic, technical and legal challenges” to IS. Lubin (2019) posits that the increased adoption of cyber insurance policies by private corporations, groups, and individuals may have a chilling effect on IS because “there are often very strict parameters regarding [a policy holder’s] notification and cooperation [regarding hostile cyber events] in the insurance policy.” Finally, the methodologies for evaluating the success of certain IS platforms over others are still developing – as are the definitions of “success” itself in the cyber context (Garrido-Pelaz, González-Manzano, & Pastrana, 2016, pp. 15–24).

The reasons that organizations may fail to fully adopt and operationalize IS, despite its advantages, may be characterized as either (1) operative or (2) normative-substantive.

The operative disincentives include:

- The inability to establish trust among sharing entities, some of whom may be competitors, including the concern regarding free riders (entities who benefit from IS without contributing themselves).
- Costs related to IS including recruitment, training and retention of appropriate cybersecurity personnel and organizational time spent on IS, including time devoted to “false positives” (i.e., incorrect alerts that are based on bad information) (Powell, 2005, p. 507).
- Lack of transparency regarding the robustness and confidentiality of IS platforms, including the possible use of shared data by any participating government agencies for noncybersecurity purposes, such as the tracking of individuals for immigration control or unauthorized surveillance (Johnson et al., 2016, pp. 4–5).
- Regulatory redundancy, where other, possibly competing, IS formats are mandated and may complicate efficient IS (Knerr, 2017, pp. 550, 553; Robinson, 2012).[13]
- Concern that participation in IS platforms may result in the perception that the sharer is vulnerable to cyber threats (Wagner et al., 2019, at 2.6).

[12] The well-known example of the 2017 breach into the Equifax credit reporting company illustrates the pitfalls that characterize the reluctance of some financial sector actors to engage effectively with IS. See Warren (2018). See also Fournoy & Sulmeyer (September/October, 2018).

[13] One leading example can be seen in the USA, where the financial sector is defined as one of the sixteen included under the aegis of DHS and also subject to the directives of the US Department of Treasury and anti-money laundering reporting requirements.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

Three of the normative-substantive disincentives are:

- The potential exposure of protected personal data shared by organizations, with resulting regulatory sanctions and exposure to litigation by data subjects and regulators.
- The potential exposure of organizational IP, with potential chilling effects on organizational innovation, and possible implications for corporate market value.
- Concerns regarding antitrust implications of IS within a sector.

Taken together, both the operative and substantive-normative disincentives to IS help to explain why some cyberspace actors are reluctant to fully adopt IS as part of their overall cybersecurity strategies on their own initiative; and when they participate, may do so less than optimally (including in situations where required to do so by regulators) (Barford et al., 2010, pp. 3–13; Sutton, 2015, pp. 113–116). Nonetheless, despite these potential weaknesses in IS platforms, there is, overall, strong continued support for their inclusion in legal, policy, and standardization initiatives, as shall be shown in the following section. Not only do the potential advantages of increased "cyber situational awareness" outweigh the disincentives but, as argued here, technological developments such as standardized reporting of cyber threat indicators, STIX and TAXII architectures, TLP, and increasingly automated IS (the "commoditization" of cyber threat indicators) signal an increasing awareness of the criticality of IS for the mitigation of cyber risk on the part of all stakeholders.

4 CHARACTERIZING THE RELATIONSHIP BETWEEN CYBER PEACE AND INFORMATION SHARING: A BEST PRACTICE AND CONFIDENCE-BUILDING MEASURE THAT LEVERAGES POLYCENTRICITY

4.1 *Information Sharing as a Best Practice in Support of Cyber Peace*

The definition of cyber peace cited at the beginning of this chapter identifies four of its aspects: clarification of "rules of the road" for setting actors' expectations and thresholds for IS; threat reduction; risk assessment; and best practices for carrying out these three tasks – all of which are supported by IS. Participants in any given IS platform agree *ex ante* to the *thresholds of nonpermissible online behavior* of hostile actors, by virtue of the triggers indicating precisely when relevant information should be shared by them and is shared with them. Typical *informational asymmetries* that have characterized cyber hostilities to the advantage of the attacker are addressed by the sharing of data, such as by those alerts referred to in the above examples of CISCP and FS-ISAC. *Risk assessment* is carried out, *inter alia*, on the basis of indicators, data, and situational evaluations received through IS.

Two additional attributes of IS that support sustainable and scalable cyber peace should be noted. First, its neutrality with respect to the typology of both attackers

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

and targets. Whether the attacker is an individual, a country, a group of criminal hackers, an inside operator, or an autonomous or semiautonomous computer – the IS alert thresholds are similar.[14] Likewise, alerts, vulnerabilities, and warnings are target neutral, and are similarly applicable in the context of state-to-state hostilities, cybercrime, terrorist activity, hacktivism, and money laundering. The second attribute is the convenient scalability of IS, as sharing technologies and protocols currently undergo standardization, automatization, and commoditization.

Work is still needed to quantify the specific advantages that IS brings as a best practice in boosting levels of cybersecurity, especially in terms of its cost effectiveness as part of the overall cybersecurity strategy of organizations and states. This much needed analysis will contribute to a better understanding of the economic aspects of sustainable cyber peace, as well.

4.2 *Beyond Best Practice: The Value of Information Sharing as a CBM*

Building on this understanding of IS as a best practice, it is argued here that IS further supports sustainable cyber peace as a CBM at the international level, among the states, international organizations, and multinational companies that are critical to ensuring global cybersecurity. The framing of IS as a CBM, rather than as a binding, substantive norm to which these entities are subject as a matter of law or policy, is beneficial to the utilization of IS platforms at the international level (Borghard & Lonergan, 2018). By sidestepping substantive multilateral commitments, IS can be more readily utilized to support cybersecurity and cyber peace. Examples where this has occurred include the UN's 2015 GGE (United Nations General Assembly, 2015), the OSCE's 2016 listing of cybersecurity CBMs (Organization for Security and Co-Operation in Europe, 2016), and the 2018 Paris Call for Trust and Security in Cyberspace (Principle 9).

CBMs were originally used in the context of the Cold War to further disarmament processes in the context of the diplomatic and political standoff between the USSR and the West. Nonmilitary CBMs have been defined more generally as "actions or processes undertaken … with the aim of increasing transparency and the level of trust" between parties (Organization for Security and Co-operation in Europe, 2013). They are "one of the key measures in the international community's toolbox aiming at preventing or reducing the risk of a conflict by eliminating the causes of mistrust, misunderstanding and miscalculation" (Pawlak, 2016, p. 133). CBMs are also critical in the global cybersecurity context and have been described as a "key tool in the cyber peacebuilder's toolkit" (Nicholas, 2017).

In a 2017 in-depth study of eighty-four multilateral and bilateral initiatives addressing the collective action challenges of cybersecurity, including treaties,

[14] Barring, of course, attacks which protected systems have been directed to ignore such as pentesting and friendly intrusions. These are not always transparent to IS participants.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

codes of conduct, agreements, memoranda and public declarations, IS was found to be included as an agreed cybersecurity measure in more than 25 percent of such initiatives (twenty-one out of the total eighty-four) (Housen-Couriel, 2017, pp. 51–52). Moreover, the analysis was able to isolate several specific elements of IS, discussed above, that were individually included in this top quarter: IS measures in general[15]; establishment of a specific national or organizational point of contact for information exchange; and sharing of threat indicators (Housen-Couriel, 2017, pp. 51–52).[16] These elements were three out of a list of a dozen CBMs that occur with sufficient frequency to be included in a "convergence of concept" with which diverse stakeholders – states, regional organizations, intergovernmental organizations, specialized UN agencies, standards organizations, private corporations, sectoral organizations, and NGOs – have incorporated into cybersecurity initiatives.[17] The study concluded that, while such cyberspace stakeholders are frequently willing to incorporate general arrangements for IS (it is in fact the leading agreed-upon cyber CBM in the initiatives that were studied), and even to specify a national or organizational point of contact, they are less willing to commit to a 24/7, real-time exchange of cybersecurity related information (Housen-Couriel, 2017, p. 67). This finding indicates a gap that should be considered in the context of further leveraging IS in the context of cyber peace.

Nonetheless, as noted above, IS as a CBM holds the advantage of bypassing the present, considerable challenges of achieving formal and substantive multistakeholder agreement on substantive cyber norms, until such time as such binding norms are legally and geopolitically practicable (Efroni & Shany, 2018; Finnemore & Hollis, 2016; Macak, 2017). A few examples of binding domestic law and international regulatory requirements for organizational participation in IS platforms do exist, such as the pan-EU regime established under the EU NIS (Directive 2016/1148), the Estonian Cybersecurity Act of 2016, and the US Department of Defense disclosure obligations for contractors when their networks have been breached. However, there are many more based on voluntary participation, such as the CISCP and FS-ISAC reviewed above, Israel's FC3, and the global CERT and CSIRT networks of 24/7 platforms for cyber threat monitoring, including the EU network of more than 414 such platforms (European Union Network and Information Security Agency, 2018).

[15] Defined as "exchange between stakeholders of information about strategies, policies, legislation, best practices, and cyber infrastructure capacity building." Forty-three out of the eighty-four included this measure.

[16] Twenty-three out of the eighty-seven included this measure, and eighteen out of eighty-four included real-time 24/7 exchange of threat data.

[17] These are: Information sharing, in general, sharing of information around cyber threats, law enforcement cooperation, protection of critical infrastructure, mechanisms for cooperation with the private sector and civil society, arrangements for international cooperation, a mechanism for vulnerability disclosure, regular dialogue, the mandating of general legislative measures, training of cyber personnel, cyber education programs, and conducting tabletop exercises.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

For the purposes of its analysis in this chapter, IS constitutes as a nonbinding CBM that also constitutes a best practice for bolstering cybersecurity and cyber peace, yet does not require a binding legal basis for its implementation. The critical issue of the use of regulatory measures, both binding and voluntary, to promote IS for optimal cybersecurity and cyber peace is, as noted above, an issue for further research.

4.3 *Leveraging Polycentricity for Effective IS*

In this section, we briefly address the advantages of a polycentric approach for effective IS. Polycentricity is an approach and framework for ordering the actions of a multiplicity and diversity of actors around a collective action problem.[18] Several scholars in the field of cybersecurity describe and analyze regulatory activity in cyberspace specifically in accordance with such an approach (Craig & Shackelford, 2015; Kikuchi & Okubo, 2020; Shackelford, 2014, pp. 88–108). Polycentricity explicitly recognizes a multiplicity of sources of regulatory authority and behavioral organization for cyber activities, including nation-state actors, private sector organizations, third sector entities, and even individuals, and it acknowledges the value of employing a diversity of measures to address the collective action problem (Elkin-Koren, 1998; Shackelford, 2014; Thiel et al., 2019).

A polycentric approach is theoretically and conceptually most appropriate for supporting IS in particular and cybersecurity overall due, *inter alia*, to its inherent stakeholder inclusiveness, flexibility with regard to types of regulatory measures, and transparency with respect to potential violations of substantive privacy rights, IP protections, and antitrust provisions (Shackelford, 2014, p. 107). Moreover, in the context of IS, a polycentric approach maximizes the potential for remedying informational asymmetries among a diversity of vetted sharers, bringing to bear a variety of perspectives and capabilities (Kikuchi & Okubu, 2020, pp. 392–393; Shackelford, 2013, pp. 1351–1352).[19] Such an approach explicitly acknowledges the complex interdependencies of all actors in cyberspace (Shackelford, 2014, pp. 99–100). Thus, a polycentric approach will optimally include on an IS platform the broadest possible

[18] Polycentricity is "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes." McGinnis (2011), pp. 171–72. See also Black (2008), p. 139 ("'Polycentric regulation' is a term which acts … to draw attention to the multiple sites in which regulation occurs at sub-national, national and transnational levels.")

[19] Specifically, key parameters include the explicit inclusion of a multiplicity and diversity of trusted participants, and a range of regulatory incentives, tools and measures employed for IS. These might encompass, *inter alia*, national laws, sectoral self-regulation, best practices, guidelines, standards, international agreements, public–private partnerships, academic and consulting reports, and other types of regulation through information sharing. On the other hand, some drawbacks to the polycentric approach include fragmentation, "gridlock," inconsistency, and "the difficult task of getting diverse stakeholders to work well together across sectors and borders."

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

range of sharers: Government regulators and agencies themselves; sectoral actors that may share information informally, as they are targeted simultaneously by malicious cyber actors; umbrella groups formed within the sector for formal and informal IS; technical experts, academic and consulting actors, providing external assessments of IS models and their effectiveness; and individuals who may share information through governmental, sectoral, or organizational channels, or through informal channels such as social media – when they experience compromised cybersecurity through their personal Internet use.

The two examples reviewed above are relatively non polycentric at present: CISCP is a public–private sector partnership that includes government agencies and companies in its membership, and FS-ISAC restricts participation even further, to private sector members only (central banks, sector regulators, and other government agencies must join the separate CERES platform). The challenges for building trust on these two platforms are significant and may continue to constitute barriers for inclusion of a broader, more diverse membership. In the context of the financial sector, especially, a more polycentric participation in IS may be encumbered at present by legal and regulatory constraints. Nevertheless, financial institutions already recognize the important potential of gathering data on unusual, detrimental activity in their networks *via* reporting by customers and suppliers – that is, individual users who access parts of the network regularly and often, and who can serve as sensors for fraudulent and hostile cyber activity such as phishing (Cyber Security Intelligence, 2017). Individual user endpoints and accounts may be among the most vulnerable points of entry into an institution's network, but they also constitute a key element for cybersecurity data gathering at the perimeter of financial institutions that, we contend, should be leveraged within IS platforms as an additional means of mitigating the informational asymmetry between the hostile actor and the targeted organization. Thus, the provision of fraud prevention alert mechanisms on the websites of banks and some other private companies, by means of which customers may provide information about phishing schemes, irregular activity in their accounts, and other suspicious activity, might be incorporated into sectoral IS platforms.[20] This growing understanding on the part of financial organizations, social media platforms, and consumer websites that much valuable information with respect to cyber risks may be garnered from individuals (including customers, employees, and suppliers) requires creative thinking around the incentivization of such IS, as well as the protection of individual privacy rights as cyber risk indicators are shared.[21]

[20] See, for example, the portals for reporting suspicious cyber activity at amazon.com (www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=GPXKBLY3LY4ZNG5H); Bank of America (www.bankofamerica.com/security-center/report-suspicious-communications/#:~:text=Forward%20any%20suspicious%20email%20or,at%20800%2D432%2D1000.); and the Internal Revenue Service (www.irs.gov/privacy-disclosure/report-phishing).

[21] A key challenge in this context is the evolution of full, mutual IS, and not only unilateral reporting of risks on the part of individuals to their banks, social media platforms, and consumer platforms.

In summary, IS is likely be most effective as best practice at the domestic level and as a CBM at the international level – when it is governed by a polycentric approach for the most efficient pooling of resources, knowledge, and experience to mitigate, counter, and respond effectively to cyber threats and events.

5 SUMMARY AND CONCLUSIONS

This chapter has aimed to show how IS platforms can serve as: arbiters of cyber expertise; the exchange of technical data; real-time coordination of defensive actions; and, perhaps most importantly, the development of trust among key stakeholders in order to mitigate the effects of hostile activities in cyberspace. The analysis has aimed to support the thesis that one of the critical elements to achieving sustainable cyber peace, indeed a *sine qua non* for its governance, is the timely utilization of credible IS platforms that allow entities targeted by hostile cyber activities to pool information, resources, and insights in order to mitigate cyber risk. Successful platforms will leverage innovative technological developments for collecting actionable cyber threat data at both the tactical, real-time level of incident response, as well as that of strategic planning for amending vulnerabilities and developing long-term defense strategies.

Moreover, even as IS modalities are included in many initiatives for promoting cybersecurity among state and nonstate actors, they have the advantage of bypassing need to achieve formal and substantive multistakeholder agreement on cyber norms that are at the core of international and domestic legal regimes for the governance of cyberspace. At the international level, many contemporary scholars note that the difficulties of surmounting normative barriers await resolution until such time as states and international organizations are prepared to act more transparently in cyberspace and forge binding international and domestic legal regimes. Eventually, in international regimes to which states and organizations formally agree – or, perhaps, more gradually through the evolution of international custom – IS may be transformed from a norm-neutral CBM into an element of states' and organizations' due diligence under international cyber law.[22]

Several issues that are beyond the present scope of this chapter invite additional research. Among them are the quantifiable, cost–benefit calculations of IS platforms as an element of cybersecurity and cyber peace; the role of regulation (including substantive legal norms) in promoting and incentivizing IS; the cumulative effects of standardization and automatization on IS processes; and a broader examination of the specific advantages of an explicitly polycentric approach to IS. IS models with respect to other global collective action problems, such as public health (especially relevant in the present COVID-19 pandemic), environmental quality, and the elimination of

[22] On aspects of due diligence in the context of international cyber law, see Tallinn 2.0, Rules 6 and 7 at 30–50, and Rule 6 at 288.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

outer space debris are also salient: A broader, comparative analysis of IS regimes for the mitigation of risk in meeting these common problems may prove fruitful.

We conclude with a note of deep appreciation for the talented and committed women and men who are the ultimate heroes of the story of cyber IS: The security analysts who mine, winnow, and share critical cyber threat indicators as a matter of course, 24 hours a day, 365 days a year, over weekends, during their holiday breaks, and from anywhere they can possibly connect up to cyberspace.

REFERENCES

Ablon, L., & Bogart, A. (2017). *Zero days, thousands of nights: The life and times of zero-Day vulnerabilities and their exploits*. RAND Corporation. www.rand.org/pubs/research_reports/RR1751.html

Alliance for Cyber Security. (n.d.). *Informationspool*. Retrieved October 24, 2020 from www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/_function/Informationspool_Formular.html;jsessionid=44A7CF329463873BACD747ABEBA5CB17.1_cid351?nn=6643342

Barford, P., Dacier, M., Dietterich, T., Fredrikson, M., Giffin, J., Jajodia, S. et al. (2010). Cyber SA: Situational awareness for cyber defense. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.), *Cyber situational awareness, advances in information security* (pp. 3–13).

Barlow, J. P. (1996). *Declaration of the independence of cyberspace*.

Barnum, B. (2014). *Standardizing cyber threat intelligence information with the structured threat information eXpression (STIX™)*. http://stixproject.github.io/about/STIX_Whitepaper_v1.1.pdf

Black, J. (2008). Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. *Regulation & Governance*, *2*(2), 137–164.

Borghard, E., & Lonergan, S. (2018). Confidence building measures for the cyber domain. *Strategic Studies Quarterly*, *12*(3), 10–49. www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-3/Borghard-Lonergan.pdf?ver=fvEYs48lWSdmgIJlcAxPkA%3d%3d

Chabrow, E. (2015, March 15). *Cyberthreat information sharing privacy concerns raised*. BankInfoSecurity. www.bankinfosecurity.com/privacy-risks-raised-over-cyberthreat-information-sharing-a-8970

Cision. (2018, June 11). *FS-ISAC launches the CERES forum: World's First Threat Information Sharing Group for Central Banks, Regulators and Supervisors*. www.prnewswire.com/news-releases/fs-isac-launches-the-ceres-forum-worlds-first-threat-information-sharing-group-for-central-banks-regulators-and-supervisors-300663921.html

Citizen Lab Reports. (n.d.). *Targeted threats*. Retrieved October 24, 2020 from https://citizenlab.ca/category/research/targeted-threats/

Convention on Cybercrime. (2001, November 23). E.T.S. No. 185.

Craig, A., & Shackelford, S. (2015). Hacking the planet, the Dalai Lama, and You: Managing technical vulnerabilities in the internet through polycentric governance. *Fordham Intellectual Property, Media & Entertainment Law Journal*, *24*(2), 381–425.

Cyber Security Intelligence. (2017, May 1). *The cyber security threats that keep banks alert*. www.cybersecurityintelligence.com/blog/the-cybersecurity-threats-that-keep-banks-alert-2392.html

Cybersecurity Act of 2018. (2018, May 23). www.riigiteataja.ee/en/eli/523052018003/consolide

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

Cybersecurity and Infrastructure Agency. (2020a, April 8). *Alert (AA20-009A): Covid-19 exploited by malicious cyber actors*. www.us-cert.gov/ncas/alerts/aa20-099a

Cybersecurity and Infrastructure Agency. (2020b, January 14). *Alert (AA20-014A): Critical vulnerabilities in microsoft windows operating system*. www.us-cert.gov/ncas/alerts/aa20-014a

Deljoo, A., van Engers, T., Koning, R., Gommans,L., & de Laat, C. (2018). *Towards trustworthy information sharing by creating cyber security alliances*. 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), 1506–1510.

Directive 2016/1148, of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the union, 2016 O.J. (L194) 1.

Efroni, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn Manual 2.0 on cyber operations and subsequent state practice. *American Journal of International Law, 112*(4), 583–657.

Elkin-Koren, N. (1998). Copyrights in cyberspace – Rights without laws. *Chicago-Kent Law Review*, 73(4), 1156–1201.

European Union Network and Information Security Agency. (2018). *Cooperative models for Information Sharing and Analysis Centers (ISACs)*. www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

Europol. (2017, December 4). *Andromeda botnet dismantled in international cyber operation*. [Press release]. www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation

Europol. (n.d.). *EC3-European cyber crime centre*. www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Europol. (2020). *Report Cybercrime Online*. www.europol.europa.eu/report-a-crime/report-cybercrime-online

FBI. (2020, May 8). *The FBI's Internet Crime Complaint Center (IC3) marks its 20th Year* [Press release]. www.fbi.gov/news/pressrel/press-releases/the-fbis-internet-crime-complaint-center-ic3-marks-its-20th-year

Finnemore, M., & Hollis, D. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *110*(3), 425–479.

Fortinet. (2017, February 14). *Cyber threat alliance expands mission through appointment of President, formal incorporation as not-for-profit and new founding members* [Press release]. www.fortinet.com/ru/corporate/about-us/newsroom/press-releases/2017/cyber-threat-alliance-expands-mission.html

Fournoy, M., & Sulmeyer, M. (2018, September/October). Battlefield internet: A plan to secure cyberspace. *Foreign Affairs*. www.foreignaffairs.com/articles/world/2018-08-14/battlefield-internet.

Garrido-Pelaz, R., González-Manzano, L., & Pastrana, S. (2016). *Shall we collaborate? A model to analyse the benefits of information sharing* [Workshop presentation]. Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security.

Gill, R., & Thompson, M. (2016). *Trust and information sharing in multinational-multiagency teams*. Springer.

Global Internet Forum to Counter Terrorism. (n.d.). *Joint tech innovation*. Retrieved October 24, 2020 from https://gifct.org/joint-tech-innovation/

Harkins, M. W. (2016). *Managing risk and information security*. Apress.

Hathaway, M. (2010, May 7). *Why successful partnerships are critical for promoting cybersecurity*. Executive Biz.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

Hausken, K. (2015). A strategic analysis of information sharing among cyber hackers. *Journal of Information Systems and Technology Management*, *12*.

He, M., Devine, L., & Zhuang, J. (2018). Perspectives on cybersecurity information sharing among multiple stakeholders using a decision-theoretic approach. *Risk Analysis*, *38*(2), 215–225.

Housen-Couriel, D. (2017). *An analytical review of and comparison of operative measures included in cyber diplomatic initiatives* (GCSC Issue Brief No. 1). Global Commission on the Security of Cyberspace.

Housen-Couriel, D. (2018). Information sharing for mitigation of hostile activity in cyberspace (Part 1). *European Cybersecurity Journal*, *4*(3), 44–50.

Housen-Couriel, D. (2019). Information sharing for mitigation of hostile activity in cyberspace (Part 2). *European Cybersecurity Journal*, *5*(1), 16–24.

International Standards Organization. (2015). *ISO/IEC 27010:2015, Information Technology – Security Techniques – Information security management for inter-sector and inter-organizational communications*. www.iso.org/standard/44375.html

INTERPOL. (n.d.). *Cybercrime*. www.interpol.int/content/download/5267/file/Cybercrime.pdf

Israel Cyber Directorate. (2019). *Israel's 'Showcase' for evaluation of cyber risks*. www.gov.il/he/departments/general/systemfororg

Israeli Government. (2015, February 15). *Resolution No. 2444, advancing the national preparedness for cyber security*.

Johnson, C., Badger, L., Waltermire, D., Snyder, J., & Skorupka, C. (2016). *Guide to cyber information threat sharing* (NIST Special Pub. 800-150). National Institute of Standards & Technology. http://dx.doi.org/10.6028/NIST.SP.800-150

Kikuchi, M., & Okubo, T. (2020). Building cybersecurity through polycentric governance. *Journal of Communications*, *15*, 390–397.

Klimburg, A. (2018). *The darkening web: The war for cyberspace*. Penguin Books.

Knerr, M. (2017). Password please: The effectiveness of New York's first-in-nation cybersecurity regulation of banks. *Business Entrepreneurship & Tax Law Review*, *1*(2), 539–555.

Lin, M. J. J., Hung, S. W., & Chen, C.J. (2009). Fostering the determinants of knowledge sharing in professional virtual communities. *Computers in Human Behavior*, *25*(4), 929–939.

Liu, C. Z., Zafar, H., & Au, Y. (2014). Rethinking FS-ISAC: An IT security information sharing network model for the financial services sector. *Communications of the Association for Information Systems*, *34*(1).

Lubin, A. (2019, September 21). *The insurability of cyber risk* [Unpublished manuscript]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3452833

Macak, K. (2016). Is the international law of cyber security in crisis? In N. Pissanidis, H. Rõigas, & M. Veenendaal (Eds.), *Cyber power* (pp. 127–140). NATO CCD COE Publications.

Macak, K. (2017). From cyber norms to cyber rules: Re-engaging states as law-makers. *Leiden Journal International Law*, *30*(4), 877–899.

Mavroedis, V., & Bromander, S. (2017). *Cyber threat intelligence model: An evaluation of taxonomies, sharing standards and ontologies within cyber threat intelligence*. IEEE 2017 European Intelligence and Security Informatics Conference, 91–98.

McGinnis, M. (2011). An introduction to IAD and the language of the Ostrom Workshop: A simple guide to a complex framework. *Policy Studies Journal*, *39*(1), 169–183.

McGinnis, M. (2016). *Polycentric governance in theory and practice: Dimensions of aspiration and practical limitations*. https://mcginnis.pages.iu.edu/polycentric%20governance%20theory%20and%20practice%20Feb%202016.pdf

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

Ministry of Finance and the Cyber Directorate. (2017, September 4). *Memorandum from the finance cyber and continuity centre (FC3)*. https://docs.google.com/viewer?url=http%3A%2F%2Fwww.export.gov.il%2Ffiles%2Fcyber%2FFC3.PDF%3Fredirect%3Dno

National Cyber Security Centre. (n.d.). *CiSP terms and conditions* (v.5). www.ncsc.gov.uk/files/UK%20CISP%20Terms%20and%20Conditions%20v5.0.pdf

Nicholas, P. (2017, June 29). *What are confidence building measures (CBMs) and how can they improve cybersecurity?* Microsoft. www.microsoft.com/en-us/cybersecurity/blog-hub/CMB-and-cybersecurity

Organization for Security and Co-Operation in Europe. (2013). *OSCE guide on non-military confidence-building measures (CBMs)*. www.osce.org/secretariat/91082

Organization for Security and Co-Operation in Europe. (2016, March). *Decision No. 1202, confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*. https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/

Ostrom, E., Chang, C., Pennington, M., & Tarko, V. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge University Press.

Ostrom, E., Chang, C., Pennington, M., & Tarko, V. (2012). *The future of the commons: Beyond market failure and government regulation*. The Institute of Economic Affairs.

Oudkerk, S., & Wrona, K. (2013). Using NATO labelling to support controlled information sharing between partners. In E. Luiijf & P. Hartel (Eds.), *Critical information infrastructures security, lecture notes in computer science* (Vol. 8328). Springer Link.

Özalp, Ö., Zheng, Y., & Ren, Y. (2014). Trust, trustworthiness, and information sharing in supply chains bridging China and the United States. *Management Science*, *60*(10), 2435–2460. https://doi.org/10.1287/mnsc.2014.1905

Paris Call for Trust and Security in Cyberspace. (2018, November 12). https://pariscall.international/en/

Pawlak, P. (2016). Confidence building measures in cyberspace: Current debates and trends. In A.-M. Osula & H. Rõigas (Eds.), *International cyber norms: Legal, policy & industry perspectives* (pp. 129–153). CCDCOE.

Powell, B. (2005). Is cybersecurity a public good? Evidence from the financial services industry. *Journal of Law, Economics & Policy*, *1*(2), 497–510.

Presidential Decision Directive PDD/NSC 63. (1998, May 22). https://fas.org/irp/offdocs/pdd/pdd-63.htm

Robinson, N. (2012). Information sharing for CIP: Between policy, theory, and practice. In C. Laing, A. Baadi, & P. Vickers (Eds.), *Securing critical infrastructures and critical control systems: Approaches for threat protection*. IGI Global.

Robinson, N., & Disley, E. (2010). *Incentives and challenges for information sharing in the context of network and information security*. European Union Network and Information Security Agency. www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing

Ruhl, C., Hollis, D., Hoffman, W., & Maurer, T. (2020). *Cyberspace and geopolitics: Assessing global cybersecurity norm processes at a crossroads*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110

Schmitt, M. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press.

Schneier, B. (2020, January 15). *Critical windows vulnerability discovered by NSA*. Schneier on Security. www.schneier.com/blog/archives/2020/01/critical_window.html

Shackelford, S. (2013). Toward cyberpeace: Managing cyberattacks through polycentric governance. *American University Law Review*, *62*(5), 1273–1364.

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press

Shackelford, S. (2014). *Managing cyber attacks in international law, business, and relations: In search of cyber peace*. Cambridge University Press.

Shackelford, S. (2016). Protecting intellectual property and privacy in the digital age: The use of national cybersecurity strategies to mitigate cyber risk. *Chapman Law Review*, 19(2), 445–482.

Shu-yun, Z., & Neng-hua, C. (2007). *The collision and balance of information sharing and intellectual property protection*. http://en.cnki.com.cn/Article_en/CJFDTOTAL-TSGL200702010.htm

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*, 154–176.

Sutton, D. (2015). Trusted information sharing for cyber situational awareness. *E & I Elektrotechnik und Informationstechnik*, 132(2), 113–116.

Thiel, A., Garrick, D., & Blomquist, W. (Eds.). (2019). *Governing complexity: Analyzing and applying polycentricity*. Cambridge University Press.

United Nations General Assembly. (2015, July 22). Report A/70/174: Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security. http://undocs.org/A/70/174

U.S. Department of Homeland Security. (2020, March 30). Bulletin SB-20-097. www.us-cert.gov/ncas/bulletins/sb20-097

U.S. Department of Justice. (2020, September 16). *Seven international cyber defendants, including "Apt 41" actors, charged in connection with computer intrusion campaigns against more than 100 victims globally* [Press Release]. www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer

Van Impe, K. (2015, March 26). *How STIX, TAXII and CyBox can help with standardizing threat information*. Security Intelligence. https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information/

Vavra, S. (2019, October 22). *Why did cyber command back off its recent plans to call out North Korean hacking?* Cyber Scoop. www.cyberscoop.com/cyber-command-north-korea-lazarus-group-fastcash/

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

Warren, E. (2018). *Bad credit: Uncovering Equifax' failure to protect Americans' personal information*. Office of Senator Elizabeth Warren. www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf

Weiss, N. E. (2015, June 3). *Legislation to facilitate cybersecurity information sharing: Economic analysis*. Congressional Research Service. No. R43821.

Wendt, D. (2019a). Addressing both sides of the cybersecurity equation. *Journal of Cyber Security and Information Systems*, 7(2).

Wendt, D. (2019b). *Exploring the strategies cybersecurity specialists need to improve adaptive cyber defenses within the financial sector: An exploratory study* [unpublished doctoral dissertation]. Colorado Technical University.

Wisniewski, C. (2020, January 23). *Looking for silver linings in the CVE 2020-0601 crypto vulnerability*. Naked Security. https://nakedsecurity.sophos.com/2020/01/23/looking-for-silver-linings-in-the-cve-2020-0601-crypto-vulnerability/

World Economic Forum. (2019). Global risks report. www.weforum.org/reports/the-global-risks-report-2019

Zheng, D., & Lewis, J. (2015). *Cyber threat information sharing*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150310_cyberthreatinfosharing.pdf

https://doi.org/10.1017/9781108954341.003 Published online by Cambridge University Press