ANALYSIS

INFORMATION SHARING FOR THE MITIGATION OF HOSTILE ACTIVITY IN CYBERSPACE: COMPARING TWO NASCENT MODELS (PART 1)

DEBORAH HOUSEN-COURIEL

Deborah Housen-Couriel's Tel Aviv-based law practice advises global and Israeli clients on strategies for regulatory planning and compliance in the areas of cybersecurity law and regulation. She teaches courses on cyber law at Hebrew University and at the Herzliya IDC and is a lead researcher at several Israeli universities. Deborah was a member of the Group of Experts that drafted Tallinn Manual 2.0; and currently serves as a Core Expert for the MILAMOS project and as Chair of a Working Group at the Global Forum on Cyber Expertise.

1. Introduction: Defining the Threat and the Opportunity

1.1 Overview

Information sharing (IS) among private sector and governmental entities can serve as an effective tool for bolstering cybersecurity and mitigating damage caused by hostile cyber incidents. It does so by bridging gaps due to information asymmetries between attackers and their targets, identifying the vulnerabilities of targeted organizations and the means to quickly mitigate these exposures, and reinforcing best practices for cyber defence, both in real time and in the long term. Yet in the absence of regulation mandating IS, private sector actors may be reluctant to share information voluntarily. Even when government regulation requires IS, private sector actors' participation may not be optimal. They attribute several drawbacks to current sharing platforms, including imperfect trust relationships among participants; a lack of transparency regarding the efficiency and confidentiality of IS measures; exposure to legal liability with respect to the information shared (i.e., protected personal data); and operational and personnel costs.

In this two-part article, we briefly analyse and compare two current IS developments in light of these overarching concerns. The first is the 2016 EU Network and Information Systems Directive (NIS) that came into effect in May 2018[1], followed by Israel's Financial Cyber and Continuity Center (IFC3) established in January 2017 (Ministry of Finance, 2017, September 4). The NIS is a mandatory regulatory framework that applies to all EU member states and,

1 Directive 2016/1148 concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L194) 1 [hereinafter NIS].

once fully transposed, will apply to a broad spectrum of organizational sectors which these states will designate the operators of essential services (i.e., energy, transport, water supply) and digital service providers[2]. Under the NIS, member states themselves are required to exchange information as part of their strategic cooperation for bolstering cybersecurity; and domestic operators and providers, including private sector actors, are required to share information through a regulatory regime of incident notification. In contrast to the NIS model, the IFC3 is a national IS platform, sector-specific and voluntary. Under both frameworks the information sharing *praxis* is currently evolving.

This article proposes that, as they are increasingly implemented, each model holds insights for the functioning of its counterpart. In the first part of the article we review IS as an element of jurisdictional cybersecurity, whether the jurisdiction is sectoral, national, or trans-national. In the second part, we analyse and compare the information sharing measures and modalities of the NIS and the IFC3 as well as some of the issues that emerge from this comparison of two nascent IS platforms. The conclusion points to two future challenges for information sharing measures, whether mandated or voluntary: the special case of IS posed by responsible disclosure of cyber vulnerabilities; and the imperative to include new stakeholders, such as individual end-users of cyber products and services, in innovative ways that ensure trusted IS relationships are maintained.

1.2 Information Sharing as an Element of Cybersecurity

As hostile cyber incidents continue to escalate globally in their prevalence, disruptiveness, and financial costs, information sharing to mitigate the impact of such hostile activity in cyberspace is one of the most widely advocated measures for increasing organizational, national, and global cybersecurity among vulnerable organizations[3]. Although not the sole means of closing organizational gaps, nor by any means a blanket remedy, it is relied upon as a key measure for bolstering cybersecurity[4]. Thus, in situations in which hostile cyber incidents have spread rapidly around the globe, such as in the May 2017 WannaCry ransomware attack, real-time IS has effectively supported coordinated responses among a wide spectrum of stakeholders, including both states and private sector actors across many regulatory jurisdictions (Chabrow, 2017, November 14; and *WannaCry Ransomware Attack*..., n/d). Moreover, strategic IS, such as that supported by Information Sharing and Analysis Centres (ISACs), can leverage the best practices of diverse stakeholders for preparedness, response, and resilience in the long term (ENISA, 2017).

As hostile cyber incidents continue to escalate globally in their prevalence, disruptiveness, and financial costs, information sharing to mitigate the impact of such hostile activity in cyberspace is one of the most widely advocated measures for increasing organizational, national, and worldwide cybersecurity among vulnerable organizations.

In particular, IS can mitigate inherent informational asymmetries with respect to cyber risk assessment and response in the rapidly-changing threat environment of cyberspace[5]. The inherently global nature and scope

2 Although the deadline for NIS transposition was set for 9 May 2018, as of this writing eleven of the 28 member states have proceeded with this process (Cyprus, Czech Republic, Estonia, Finland, Germany, Italy, Malta, Slovakia, Slovenia, Sweden, and the UK). See European Commission. (2018, May 4); and European Commission. (2018, July 19).

3 On the escalation of cyber threats, see World Economic Forum. (2018). IS for increased cybersecurity is widely seen as critical across all sectors and industries (see Deloitte and Fraunhofer. (2013)). "Cybersecurity" is defined for present purposes as the process of implementing actions for the identification, prevention, mitigation, investigation, and handling of cyber threats and incidents in a digitized network; for the reduction of their effects on the network; and for the network's increased resilience in the wake of such threats and incidents.

4 "*Cyber threat information sharing is not a cure-all solution, but it is a critical step toward improving cyber defenses. The benefits of information sharing, when done correctly, are numerous. Sharing enables organizations to enhance their cyber defenses by leveraging the capabilities, knowledge, and experience of a broader community. It can provide better situational awareness of the threat landscape, including a deeper understanding of threat actors and their tactics, techniques, and procedures (TTPs), and greater agility to defend against evolving threats. It can improve coordination for a collective response to new threats and reduce the likelihood of cascading effects across an entire system, industry, sector, or across sectors.*" (Zheng and Lewis, (2015), at 1).

5 These asymmetries may exist at several levels: as between the hostile attacker and the vulnerable organization; as between governmental actors and private sector actors; and among private sector actors possessing varying risk assessment capabilities (Gibbs, Shanks, and Lederman, 2005).

of cyber activities, including hostile incidents, means that cyber threats, risks and exposures are interconnected. Thus, effective inter-organizational and cross-boundary responses depend upon reliable, relevant, and timely information sharing. The operative benefits of IS are manifested most clearly around hostile cyber events or incidents[6], yet information sharing is also crucial as an ongoing activity, independent of any specific cyber event. Analyst Sean Barnum explains the strategic criticality of IS among private sector entities:

'[N]o organization in and of itself has access to an adequate scope of relevant information for accurate situational awareness of the threat landscape. *The way to overcome this limitation is via sharing of relevant cyber threat information among trusted partners and communities.* Through information sharing, each sharing partner can potentially *achieve a more complete understanding of the threat landscape* not only in the abstract but also at the level of what specifics they can look for to find the attacker' (Barnum, 2014).

Furthermore, Tyler Moore has connected the informational asymmetry among organizations facing similar cyber threat vectors to their under-investment in cybersecurity: lack of risk awareness will likely result in a shortfall of resources devoted to risk mitigation (Moore, 2010; and Gordon, Loeb, and Lucyshyn, 2003).

What is information sharing for cybersecurity? For the purposes of this article it is defined as the exchange of information that promotes organizational and collective cybersecurity, encompassing data on cyber risks, threats, and incidents – especially hostile incidents – and the operational responses to them. IS may take place among private sector organizations, and between them and government regulators. The information shared includes *administrative and business continuity data* (threat intelligence and analysis), *technical indicators* (alerts, indicators of potentially hostile events or the behaviour of a certain hostile actor); *operative information* on practical

What is information sharing for cybersecurity? It is defined as the exchange of information that promotes organizational and collective cybersecurity, encompassing data on cyber risks, threats, and incidents – especially hostile incidents – and the operational responses to them. IS may take place among private sector organizations, and between them and government regulators.

6 Such an incident may be defined as *'an event which changes the security posture of an organization or circumvents security polices developed to prevent financial loss and/or the destruction, theft, or compromise of proprietary information. Also, an event investigated by an organization due to unusual activity, that cannot be explained as a consequence of normal operations.*" (CSIRT, n/d). See also the definition of "incident" in Article 4 (7) of the NIS.

measures for mitigating hostile cyber activity through network defence (tool configurations); and *protected information* such as personal data or organizational intellectual property (Johnson et al., 2016)[7]. Increasingly, IS may also encompass *responsible disclosure of cyber vulnerabilities*, a topic beyond the scope of this analysis and noted in the conclusion as one of the developing challenges for IS platforms[8].

Some well-known examples of cybersecurity information sharing platforms and consortia that operate on a global basis include Computer Emergency Response Teams (CERTs)[9], Computer Security Incident Response Teams (CSIRTs)[10], the Forum of Incident Response and Security (FIRSTs)[11], the Cyber Threat Alliance, and the US-initiated Information Sharing and Analysis Centres (ISACs) and Cyber Information Sharing and Collaboration Program (CISCP)[12]. These and other platforms utilize a growing diversity of coordinated communications protocols to relay relevant data and indicators among participants[13]. Platforms and protocols may also be specified by IS regulation applicable in a particular jurisdiction: one example discussed at greater length herein is the specification of CSIRT platforms in the EU NIS Directive[14]. Participation of private sector organizations in specific IS platforms available in a given jurisdiction may be either required by government regulation or voluntary (Bedrijfsrevisoren, De Muynck and Portesi, 2015). Although the scope of the present analysis does not permit a full treatment of these diverse regulatory regimes (Gibbons, 1997; and Nolan, 2015)[15], the two chosen for analysis herein represent these two modalities.

2. The Challenge of Private Sector Ambivalence

Despite the advocacy of IS by many theorists, regulators, and practitioners, some private sector organizations continue to approach it with ambivalence (Aviram and Tor, 2004). This is because exchanges that bring real value to participants require trusted interactions that reveal potential or actual organizational vulnerabilities, operational preparedness and response capabilities, and sharing of data processed by the organization. Yet where regulation does not compel IS, private sector actors may opt out of voluntary sharing[16]. Even when sharing is mandated by a regulator, and when government agencies contribute their own knowledge of cyber threats and risks for the benefit of all participants, private sector actors' participation may be less than optimal (Kopp, Kaffenberger and Wilson, 2017). They attribute several drawbacks to current information sharing platforms, which may be characterized as operative or normative. The *operative reasons* include challenges such as:

- *Imperfect trust relationships* among participants, who may be market competitors;
- *Lack of transparency regarding the efficiency and confidentiality of IS platforms*, including the use of shared data by any participating government agencies for non-cybersecurity purposes (Johnson et al., 2016);
- *Undue exposure of organizational vulnerabilities, preparedness and response measures;*
- *Costs related to IS* including recruitment, training, and retention of appropriate personnel; and organizational time spent on IS, including time devoted to "false positives" (Powell, 2005; Etzioni, 2014; and Gordon, Loeb, and Lucyshyn, 2003).

7 For present purposes, IS does not include first-level exchanges with military or covert state actors, although such actors may indirectly share via other government entities.

8 See, for example, CERT Guide to Coordinated Vulnerability Disclosure (2017).

9 See US-CERT. (n/d).

10 See ENISA. (2016).

11 See FIRST. (n/d).

12 See Cyber Threat Alliance. (2014).

13Among these are the Incident Object Description Exchange Format (IODEF), Traffic Light Protocol (TLP), Structured Threat Information eXpression (STIX), Trusted Automated eXchange of Indicator Information (TAXII), Cyber Observable eXpression (CybOX) and the DHS Automated Indicator Sharing (AIS) (Van Impe, 2015, March 26; and DHS, n/d).

14 See NIS Articles 9 and 12. For cyber event taxonomies for CSIRTs, see ENISA. (2018).

15 The 2015 US Cybersecurity Information Sharing Act is one example, stipulating that one of the aims of such sharing is "...[t]o detect, prevent, or mitigate cybersecurity threats or security vulnerabilities..." (Cybersecurity Information Sharing Act, 2015).

16 The issue of market failure as it impacts cybersecurity is not within the scope of this article, although it does constitute a critical impetus for regulatory intervention for IS.

Normative challenges include:

- *Exposure to legal liability* with respect to protected personal data and intellectual property, either entrusted by others to the organization or developed internally; and
- Concerns of susceptibility to *antitrust claims* flowing from IS[17].

Because of the present financial, disruptive, and reputational costs of hostile cyber activity for both governmental and private sector stakeholders, the stakes are high for achieving a clearer analytical understanding of how to incentivize IS for all actors. Both operative and normative drawbacks, whether actual or perceived, need to be addressed by IS platforms that are concerned with their own sustainability and effectiveness (Vazquez et al., 2012). Moreover, the challenges of the current cyber threat landscape require not only agreement on the part of organizational actors that IS strengthens cybersecurity and resiliency for all, but also the development of a high level of mutual trust among these actors (Nelson, 2017). Overall, many practitioners and regulators are seeking to improve IS mechanisms and support private sector buy-in and participation in order to better leverage IS as a critical factor for mitigating hostile activity in cyberspace (Johnson et al., 2016; and Bedrijfsrevisoren, De Muynck and Portesi, 2015, p. 6)[18].

Because of the present financial, disruptive, and reputational costs of hostile cyber activity for both governmental and private sector stakeholders, the stakes are high for achieving a clearer analytical understanding of how to incentivize IS for all actors.

3. Comparing the EU NIS and the IFC3

In this second part of this article, we will review and analyse two relatively new initiatives that aim to promote jurisdictional cybersecurity among private sector and government stakeholders through the inclusion of IS platforms as an integral, strategic element of overall preparedness, response and resilience. Comparison between the EU's NIS-mandated platform for IS and Israel's Cyber and Finance Continuity Center (FC3) requires methodological caution, as the regulation supporting each initiative differs in nature and applicability in their respective jurisdictions. Nonetheless, we propose that, as each of these nascent platforms develops a *praxis* for IS, they may mutually benefit from the experience of their counterpart. ■

17 For example, see a discussion of normative liability issues under the 2015 US Cyber Security Information Act see Schwartz, A. et al. (2017).

18 On IS measures in multilateral agreements and initiatives, see Housen-Couriel, D. (2017).

REFERENCES

Aviram, A. and Tor, A. (2004). Overcoming Impediments to Information Sharing. *55 Ala. L. Rev. 231*.

Barnum, S. (2014). Standardizing cyber threat intelligence information with the structured threat information expression. pp. 5-6.

Bedrijfsrevisoren, D., De Muynck, J, and Portesi, S. (2015). Cyber security information sharing: an overview of regulatory and non-regulatory approaches. *ENISA*. pp. 6-10.

Chabrow, E. (2017, November 14). How Information Sharing Helped Curtail WannaCry Harm. *BankInfo Security*. Retrieved from: https://www.bankinfosecurity.com/interviews/how-info-sharing-helped-curtail-wannacry-harm-in-us-i-3772

CSIRT. (n/d). Definition of an incident. Retrieved from: http://www.csirt.org/incident_report/index.html

Cyber Threat Alliance. (2014). A new way to share threat intelligence.

Cybersecurity Information Sharing Act. (2015). S. 754, 114th Cong. Title I, Sec. 104.

Deloitte and Fraunhofer. (2013). Cybersecurity: The perspective of information sharing.

Department of Homeland Security. (2018, August 31). Cyber Information Sharing and Collaboration Program (CISCP). Retrieved from: https://www.dhs.gov/ciscp

Department of Homeland Security. (n/d). Automated Indicator Sharing (AIS). Retrieved from: https://www.dhs.gov/ais

ENISA. (2016). CSIRT capabilities: How to assess maturity? Guidelines for national and governmental CSIRTs.

ENISA. (2017). Information Sharing and Analysis Centers (ISACs): Cooperative Models.

ENISA. (2018). Reference incident classification taxonomy.

European Commission. (2018, May 4). *State of play of transposition of the NIS Directive*. Retrieved from: https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.

European Commission. (2018, July 19). Commission asks Member States to transpose into national laws the EU-wide legislation on cybersecurity. Retrieved from: https://ec.europa.eu/digital-single-market/en/news/commission-asks-member-states-transpose-national-laws-eu-wide-legislation-cybersecurity

Etzioni, A. (2014). The Private Sector: A Reluctant Partner in Cybersecurity. *15 Geo J. Int'l Aff.* 69.

FIRST. (n/d). FIRST Malware Information Sharing Platform (MISP) instance. Retrieved from: https://www.first.org/global/sigs/information-sharing/misp

GFCE. (2017). CERT Guide to Coordinated Vulnerability Disclosure. *Global Good Practices: Coordinated Vulnerability Disclosure*.

Gibbs, M. R., Shanks, G. and Lederman. R. (2005). Data Quality, Database Fragmentation and Information Privacy. Surveillance and Soc. 45

Gibbons, L. J. (1997). Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace. *6 Cornell J.L. & Pub. Policy*. 475.

Gordon, L., Loeb, M. and Lucyshyn, W. (2003). Sharing Information on Computer Systems Security: An Economic Analysis. *22 J. Acct. & Pub. Policy*. pp. 461-485.

Hartman, B. et al. (2012). Breaking Down Barriers to Collaboration in the Fight Against Advanced Threats. RSA Security Brief. Retrieved from: https://www.emc.com/collateral/industry-overview/11652-h9084-aptbdb-brf-0212-online.pdf

Housen-Couriel, D. (2017). An Analytical Review and Comparison of Operative Measures Included in Cyber Diplomatic Initiatives. GCSC Issue Brief 1. pp 46-84.

Johnson, C., et al. (2016). NIST Guide to Cyber Information Threat Sharing. *Special Publication. 800-150*.

Kopp, E., Kaffenberger, L. and Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability. pp 6-8.

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

Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options. *3 Int. J. Crit. Infrastructure Prot.* 103. p. 8.

Nelson, B. (2017). The Value of Information Sharing. *The Clearing House*. Retrieved from: https://www.theclearinghouse.org/research/banking-perspectives/2017/2017-q2-banking-perspectives/the-value-of-information-sharing.

Nolan, A. (2015). Cybersecurity and Information Sharing: Legal challenges and Solutions. *Cong. Research Serv., R43941*.

Powell, B. (2005). Is Cybersecurity a Public Good? Evidence from the Financial Services Industry. *1. J. L . Econ. & Policy. 497*. p. 507.

R. Gibbs, M., Shanks, G., & Lederman, R. (2005). Data Quality, Database Fragmentation and Information Privacy, *3 Surveillance & Soc.*

Richet, J-L. Market Failure Mechanisms in Cybersecurity. *WISP Proceedings 2012*. p 26.

Schwartz, A. et al. (2017). Automatic Threat Sharing: How Companies Can Best Ensure Liability Protection When Sharing Cyber Threat Information with Other Companies or Organizations. *50 U. Mich. J. L . Reform 887*.

US-CERT. (n/d). Information Sharing Specifications for Cybersecurity. Retrieved from: https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity.

Van Impe, K. (2015, March 26). How STIX, TAXII and CyBox Can Help with Standardizing Threat Information. *Security Intelligence*.

Vazquez, D. et al. (2012). Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships. *4th International Conference on Cyber Conflict, CCDCOE*. [eds. C. Czossek, R. Ottis, K. Ziolkowski].

WannaCry Ransomware Attack and International Information Sharing. (n/d). Retrieved from : https://www.billingtoncybersecurity.com/wannacry-ransomware-attack-international-information-sharing/.

World Economic Forum. (2018). *Global Risk Report*.

Zheng, E. and Lewis, J. A. (2015). Cyber Threat Information Sharing: Recommendations for Congress and the Administration. Center for Strategic and International Studies.

ANALYSIS

Information Sharing for the Mitigation of Hostile Activity in Cyberspace: Comparing Two Nascent Models (Part 2)

DEBORAH HOUSEN-COURIEL, ADV.
THE HEBREW UNIVERSITY
CYBER SECURITY CENTER

1. Recapping: Information Sharing as an Element of Cybersecurity

In the first section of this two-part article (Housen-Couriel, 2018), we argued that information sharing (IS) among private sector and governmental entities can serve as an effective tool for bolstering cybersecurity and mitigating damage caused by hostile cyber incidents. Nonetheless, in the absence of regulation mandating IS, private sector actors may be reluctant to share information voluntarily; and even when government regulation requires IS, private sector actors' participation may not be optimal. The drawbacks they currently ascribe to IS platforms include imperfect trust relationships among participants; a lack of transparency regarding the efficiency and confidentiality of the IS process; exposure to legal liability with respect to the information shared (i.e. protected personal data or intellectual property); and operational and personnel costs related to participation in IS platforms (ENISA, 2017).

In the second part of this two-part article, we briefly analyse and compare two current IS developments in light of these overarching concerns. The first is the 2016 EU Network and Information Systems Directive (NIS) that came into effect in May 2018[1]; and the second is Israel's Cyber and Finance Continuity Center (IFC3), established in January 2017 as a joint initiative of the Ministry of Finance and the Cyber Directorate (Ministry of Finance, n.d.; Ministry of Finance, 2017, September 4). NIS is a mandatory regulatory framework that applies to all EU member states and, once fully transposed, to a broad spectrum of organisational sectors in which states designate the operators of essential services (i.e. energy, transport, water supply) and to digital service providers[2].

1 Directive 2016/1148 concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 OJ (L 194/1) [hereinafter NIS].

2 The deadline for NIS transposition was set for May 9, 2018: as of this writing 12 of the 28 member-states have taken action (Cyprus, Czech Republic, Estonia, Finland, Germany, Italy, Malta, Netherlands, Slovakia, Slovenia, Sweden, UK). See European Commission. (2018, May 4).

Under the NIS, member states are required to exchange cybersecurity-related information on an ongoing basis; and domestic operators and providers, including private sector actors from seven diverse sectors, are required to share information through a regulatory notification regime. In contrast to the NIS model, the IFC3 is a national IS platform, specific to the financial sector, and voluntary.

In the first part of the article we examined IS as a measure that contributes to optimal jurisdictional cybersecurity, whether the jurisdiction is sectoral, national, or trans-national. In this second part, we analyse and compare the IS measures and modalities of NIS and the IFC3 as well as several issues that emerge from their comparison. The conclusion points to two key future challenges: (a) the special case of IS arising from responsible disclosure of cyber vulnerabilities; and (b) the imperative to include new stakeholders, such as individual end-users of cyber products and services, in innovative ways that maintain trusted IS relationships.

2. Comparing the EU NIS and the IFC3

The two nascent initiatives aim to bolster cybersecurity in their respective jurisdictions through IS among governmental bodies and private sector organisations[3]. They do so by promoting IS as an integral, strategic element of overall preparedness and resilience. Under both frameworks the information sharing *praxis* is currently evolving. Nevertheless, we propose that as they are increasingly implemented, each model holds insights for the functioning of its counterpart.

3. Information sharing under the EU NIS Directive

The EU has moved ahead in recent years with several key regulatory developments to increase cybersecurity, including its 2013 Cybersecurity Strategy (European Commission, 2013, February 7), the 2016 Communication on Cyber Resilience (European Commission, 2016, July 5), the GDPR[4], and upgraded authorities for the European Agency for Network and Information Security (ENISA)[5]. In the context of these developments, the NIS Directive entered into force in August 2016 with a deadline of May 9, 2018 for transposition into national laws of member states (NIS, 2016, Article 25)[6]. The directive establishes a pan-EU framework for regulatory measures and technical requirements to support IS among relevant state and private sector actors to counter cyber risks and hostile incidents, while safeguarding protected personal data and other protected data types (ETSI, 2017, p. 7).

The goal of the NIS is to achieve a high common level of network and information security among member states by requiring them to implement a basket of common measures for cooperation at two interlocking levels: (a) the multilateral EU plane; and (b) within member states' domestic jurisdictions (ETSI, 2017, pp. 5-6)[7].

3 At present, the latter include only commercial enterprises. By way of contrast, there are information-sharing platforms that include universities, non-profit organisations and individuals as participants, such as Luxembourg's MISP – Malware Information Sharing Platform (www.misp-project.org), the UK's Threatvine (www.sure-vine.com/threatvine/), and Australia's Joint Cyber Security Centres (www.cert.gov.au/jcsc/jcsc-partners).

4 Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 OJ (L 119/1).

5 Regulation (EU) 526/2013 of 21 May 2013 concerning the European Union Agency for Network and Information Security, 2013 OJ (L 165/ 41).

6 See the status of transposition by member states in the references at supra note 2.

7 These measures include: adoption of a *national information security strategy*; establishment of a *Cooperation Group* to coordinate implementation; establishment of *national competent authorities* and *single points of contact*; the obligation of states to designate the abovementioned "operators of essential services" and "digital service providers"; states' obligation to enforce incident notification and other requirements; establishment of a network of CSIRTs; implementation of cyber risk management practices and controls; and international cooperation promoting a global approach to standards and information exchange.

IS constitutes a key element at both the EU and national levels and is established to support the overarching NIS goals for cyber incident management and response, as well as building trust among stakeholders. The key paradigm is that of "structured information sharing" regarding incidents and risks, implemented at both the EU and national levels (ETSI, 2017, pp. 6, 11-12). NIS establishes two types of IS through notification: compulsory and voluntary.

3.1 Compulsory notification requirements

The first IS context is the compulsory notification requirement for cyber incidents having a "significant impact" that devolves upon designated operators of essential services, and a similar "substantial effect" for digital service providers[8]. Articles 14 and 16 of the NIS Directive set out this requirement in similar language, as follows:

> Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact ["substantial impact", for digital service providers] on the continuity of the essential services they provide [or on the provision of a service they offer]. Notifications shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident. Notification shall not make the notifying party subject to increased liability.

This provision is applied in the first instance within a national jurisdiction, and thus determines the significance or substance of the impact of a given incident subject to the common NIS criteria provided in Articles 14(4) and 16(4). The national competent authority or CSIRT then determines whether the information should be shared with other EU member states. At this second level of trans-national IS among EU members, explicit substantive constraints on IS apply, as follows:

- The information exchanged is limited to data which is *relevant and proportionate* to the purpose of the IS (NIS, 2016, Article 1(5); 12(3)(b) and (c); Recitals 40-41);
- The *confidentiality* of information is preserved, as are the *security and commercial interests* of operators and providers (NIS, 2016, Article 1(5); 12(3)(b) and (c); Recitals 40-41);
- *GDPR safeguards apply* with respect to IS of personal data (NIS, 2016, Article 2);
- IS takes place without prejudice to *essential national security interests* under Article 346 of the TFEU (NIS, 2016, Article 1(5));
- Trans-national IS carries forward the *exemption from increased liability* for the notifying party specified in Articles 14 and 16.

3.2 Voluntary IS

The second context is *IS through voluntary notification*[9]. This mode of information sharing is established under NIS Article 20 for "any reasonably identifiable circumstance or event having a potential adverse effect on the security of networks and information systems…" (ETSI, 2017; NIS, 2016), as follows:

> [E]ntities which have not been identified as operators of essential services and are not digital service providers may notify, on a voluntary basis, incidents having a significant impact on the continuity of the services which they provide.

The same explicit legal constraints apply to voluntary notification as have been specified above, with respect to compulsory notification requirements (NIS, 2016, Article 20(1)). Thus, some of the normative challenges for private sector participants for voluntary IS that were noted in section 2 above have been addressed explicitly within NIS, with

8 See the criteria for determining "significant impact" in NIS Article 14(4) and "substantial impact" in NIS Article 16(4); and Annexes II and III and Recitals 9-20 on criteria for member states' to designate their operators of essential services and digital service providers.

9 There is a certain overlap of the two contexts, for example in NIS Article 14(5). For the reporting procedures on the part of operators and service providers, see Articles 6,14-17. In this context the NIS adopts the terminology of "information exchange" rather than IS, to which it refers exclusively in the context of preserving trusted legacy IS mechanisms (NIS Article 5 and Recitals 35 and 59).

safeguards provided by commercial confidentiality and personal data protection specifically incorporated. Moreover, entities that opt for voluntary notification do not incur any of the additional responsibilities that may follow from obligatory notification, such as being required to notify the public regarding a specific cyber incident[10].

Finally, the modes of implementation of IS in both the obligatory and voluntary contexts are described in NIS Articles 8-13. The national competent authorities are charged with this responsibility through their participation in the Cooperation Group (NIS, 2016, Article 11); and the requirement that they designate a national CSIRT to participate in the pan-EU CSIRT network[11]. The CSIRTs themselves are charged with operative IS which is, for the present, voluntary for private sector stakeholders unless their participation is compelled by other, non-NIS regulation[12]. 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 to stakeholders; as well as support for incident response.

Although the NIS has only recently come into force, the mandated IS platforms are already in place and operational: and the directive is likely to incentivise and optimise participation in these existing IS platforms.

In summarising this brief look at IS under the NIS, we emphasise the explicit substantive safeguards that obtain at both the national and trans-national levels: the confidentiality of shared information is preserved, as are the security and commercial interests of sharing entities and their exemption from any increased liability. Moreover, at the practical level, the inclusion of CSIRTs as the operational infrastructure of this directive builds existing IS capabilities into the new legal framework: all EU member states currently have CSIRTs (or similar CERTs) in place (ENISA, n.d., p. 25). The NIS promotes a formalisation of their mandate and operations as part of the pan-EU IS infrastructure. Moreover, ENISA has initiated a CSIRT assessment program in the NIS framework, including an EU-wide accreditation scheme (ENISA, 2016, p. 25). Thus, although the NIS has only recently come into force, the mandated IS platforms are already in place and operational: and the directive is likely to incentivise and optimise participation in these existing IS platforms (Katulić, 2018).

4. Information sharing at Israel's IFC3

4.1 Regulatory background: an absence of obligatory IS

Israel's regulatory engagement with various aspects of cybersecurity at the national level began relatively early in the mid-1990s with several legal initiatives, including the Computers Law of 1995, the Law for Regulating Security in Public Bodies of 1998 and Resolution B/84 of the Ministerial Security Committee Decision of 2002 (Tabansky and Ben Israel, 2015). A major focus on a national strategy, institutional preparedness and workforce development began with the August 2011 government resolution No. 3611 entitled *Advancing National Cyberspace Capabilities* and establishing the National Cyber Bureau (NCB) as the lead governmental agency for cybersecurity policy coordination[13]. Two subsequent government resolutions followed in 2015, *Advancing National Regulation and Governmental Leadership in Cyber Security* (No. 2443) and *Advancing the National Preparedness for Cybersecurity* (No. 2444) to promote specific elements of national

10 "Voluntary notification shall not result in the imposition upon the notifying entity of any obligations to which it would not have been subject had it not given that notification", NIS Article 20(1).

11 NIS Article 12. The national CSIRT must be provided with adequate support for fulfilment of its tasks (NIS Article 9).

12 See, for instance, NIS Article 1(7).

13 Among the goals of this initial government resolution were "to advance coordination and cooperation" among government bodies and other sectors, to produce an annual document on cyber threat vectors, and to publish "warnings and information for the public regarding cyber threats", yet these aims stop short of full information-sharing measures (Government Resolution 3611, 2011, August 7).

cybersecurity, including the establishment of a national CERT and the first references to IS measures (Housen-Couriel, 2017). Resolution 2443, which addresses internal government measures, mandates development of "processes for information sharing inside the government, including reporting to the National CERT" (Government of Israel, 2015a, Article 3c of Addendum E). The complementary Resolution 2444, which addresses the Israeli cyber ecosystem as a whole, charges the National Cyber Bureau with establishing, together with the National Cyber Authority:

> A national technological and organisational infrastructure for early warning, analysis, alert and sharing of information, in order to expose and identify cyberattacks on the State of Israel. This will be in accordance with the recommendations to be formulated [...] with regard to aspects related to the establishment of this infrastructure [...] *including the scope of information to be collected, the format of its use, and how it is to be protected and shared*. (Government of Israel, 2015b, Article 5)[14].

Thus, Resolution 2444 explicitly mandates the establishment of a national IS mechanism, although it refrains from imposing a regulatory requirement on organisations for information sharing or notification. Indeed, at present there are no compulsory IS measures for cybersecurity in Israel that are imposed on private sector entities by national legislation[15]. Some notifications are required by certain entities that are classified as critical infrastructure, although such notifications are largely not transparent to the public and are not categorised as IS for present purposes (Haber and Zarsky, 2017)[16].

4.2 Information-sharing developments in the financial sector

Nonetheless, interesting developments with respect to sectoral information sharing are evident in two promulgated directives that relate to IS in the banking and financial services sectors. The first is the Bank of Israel's March 2015 Cyber Defense Management Directive No. 361, which provides that "[t]he banking corporation shall share information that may help other banking corporations in handling cyber threats" (Bank of Israel, 2015), *via* modalities which will be determined by future directives that have yet to be published at the time of this writing. The second is the Supervisor of Capital Markets' August 2016 Directive on the Management of Cyber Risks, which prescribes an obligation on financial sector organisations only to *consider* sharing information with Israel's national CERT that may be relevant to cyber risk or to operative situations (Supervisor of Capital Markets, 2016, Article 5(a)(1)(b))[17]. A third relevant regulatory development for information sharing is the March 2017 Public Statement issued by Israel's Antitrust Authority, providing clarification on IS for cybersecurity for all Israeli organisations and exempting such IS from antitrust sanctions when certain conditions are fulfilled (Antitrust Commissioner, 2017).

Thus, despite this lack of any formal, compulsory regulatory requirements prescribing the parameters and modalities of IS for Israel's financial sectors, sectoral interest in a viable IS platform has been awakened and has motivated a high level of participation in voluntary IS through IFC3. We propose that this interest may also be motivated

14 See also Article 2 on the National Cyber Authority's responsibilities with respect to fostering cooperation among various sectors.

15 Such compulsory measures have been included in a proposed bill for Israel's national cybersecurity law of June 2018 (Government Bill on Cybersecurity and the National Cyber Directorate 2018 (in Hebrew), at 40 and Articles 16, 17, 65 and 66). Moreover, in the explanatory notes to the Bill there is an explicit reference to the NIS provisions for IS (at 15).

16 Critical infrastructure systems are subject to IS requirements that are largely non-transparent. There are also regulatory requirements to notify the data privacy regulator about certain incidents under Article 11 of the Privacy Protection Regulations (Data Security) 5777-2017, and the Israel Stock Exchange about risks and incidents that may have a significant impact on a company or its share price (Article 36, Securities Regulations (Periodic and Immediate Reports), 5730-1970).

17 Reporting to the Supervisor of Capital Markets is required only for two types of "significant" incidents (Article 5(a)(11)). *See also* the support given by the Capital Markets Supervisor for the contribution of IS to cybersecurity following an audit of cybersecurity in this sector (Supervisor of Capital Markets, *Results of a Cyber Audit*, 8.7.2018. (in Hebrew)).

by the need to comply with other required elements of the Bank of Israel and Capital Markets directives, IS having become increasingly critical to effective organisational compliance to these other stipulations.

4.3 The establishment and operation of IFC3

In January 2017 the Israeli government established the Cyber and Finance Continuity Center (IFC3) under the joint aegis of the Ministry of Finance's Cyber, Emergency and Security Division and the Cyber Directorate (Weis, 2017, September 17). These two government regulators currently operate IFC3, which is located on the premises of Israel's national CERT in the southern city of Beersheba. At present, around forty organisations voluntarily participate in the IS platform on the basis of CERT-IL's declaration of operating principles and a non-disclosure agreement to which each organisation has adhered (National Cyber Authority, n.d.). They include all major banks, credit card firms, financial services firms, financial trade associations, and financial utilities and insurance companies (Ministry of Finance, 2017, September 4).

The IFC3 divides its IS capabilities into four areas: general cybersecurity, cyber fraud, business continuity, and innovation (Weis and Shtokhamer, 2017, June 25; Shtokhamer, 2018, June 19). In its first six months of activity, IFC3 prepared and distributed to its members 120 alerts based on shared information; dealt with 45 sectoral hostile cyber events, including the WannaCry ransomware attack in May 2017; and conducted a cyber exercise together with similar centres outside Israel (Weis and Shtokhamer, 2017, June 25).

The response of IFC3 to the WannaCry events, in particular, exemplified the importance of sector-wide IS and response coordination. FC3 had shared information to its participants on the Shadow Brokers group April 2017 leak of NSA vulnerabilities that were eventually used in the WannaCry attack a month later. The situation was monitored on an ongoing basis until the beginning of the attack on May 12, when members shared information through the automated system used by the platform for real-time indicators, including operative cyber-defence indicators, and participated in a WannaCry simulation to examine their own vulnerabilities during unfolding events.

The response of IFC3 to the WannaCry events, in particular, exemplified the importance of sector-wide IS and response coordination.

The outcome of a relatively low rate of WannaCry impact on the Israeli financial sector cannot be attributed solely to the IFC3 platform's IS, yet participants have stated that the IS measures were effective in real-time and it may have been a contributing factor (Weis and Shtokhamer, 2017, June 25). The high level of *de facto* participation in the WannaCry simulation and the IS around actual events is attributed to the trusted environment that has demonstrated its reliability and value to users over a relatively short period of time (Weis, 2017, September 17).

5. Analysis and insights

In comparing the EU's NIS-mandated platform for IS and Israel's IFC3 it is clear that both models use IS as part of a broader jurisdictional and policy approach to cybersecurity. Their comparison and analysis below address three aspects:

- **Formal regulatory requirements v. voluntary participation**

The EU has taken a more formally regulated approach that provides for relatively complex institutional interaction (Cooperation Council, 28 national competent authorities, points of contact, and a network of CSIRTs). It also requires national legislation for its full implementation. In contrast, Israel has yet to regulate mandatory IS at the level of national legislation: government decisions, sectoral directives, and some second-tier regulation, including CERT-IL's declaration of operating principles, constitute its current provisions in this matter.

- **Scaling up: intra-sectoral, inter-sectoral and inter-jurisdictional IS**

It may be argued that the IFC3 model more readily bolsters trust relationships because of the smaller number of participants than those in the national CERTs and pan-EU IS mechanisms. The sectoral model provides sharers with a common professional language, understanding of risk and regulatory constraints; and professional networks and connections may ease voluntary participation in an IS platform[18]. NIS may be able to leverage this IFC3 advantage by eventually "sectoralising" its CSIRT network; on the other hand, the IFC3 stands to gain by scaling up to collaborate across other Israeli sectoral lines[19]. In accordance with the network advantages that can be gained by inter-jurisdictional IS, both models incorporate mechanisms for such sharing, although they are beyond the scope of the present analysis (NIS, 2016, Article 13; National Cyber Authority, n.d.).

- **Substantive constraints on IS**

NIS provides a key element missing from the Israeli model: explicit substantive constraints with respect to the relevance and proportionality of IS, confidentiality and data protection, and the limitation of liability for sharers. These important constraints are likely to contribute to the long-term credibility of the NIS platform, as sharers can better understand the parameters of their participation, calibrate expectations, and have recourse should such issues arise. The IFC3 currently relies upon two informal documents for elaboration of these constraints, the Antitrust Authority's Public Statement of March 2017 and the *CERT Operating Principles*. Although it may at present be able to resolve these considerations "in-house", by leveraging the trust relationships that have developed through utilisation of the platform and its reliability, it is critical for Israel's evolving IS platforms – IFC3 and others – that overarching principles and legal constraints be in place transparently and at the legislative level for this evolution to proceed in an optimal manner[20].

In comparing the EU's NIS-mandated platform for IS and Israel's IFC3 it is clear that both models use IS as part of a broader jurisdictional and policy approach to cybersecurity.

6. Conclusions and next challenges

As discussed in the first part of this article, differing approaches to the regulation of IS platforms have an impact on their effectiveness. In particular, the ways in which government actors and private sector entities interact for IS and whether interactions are obligatory or voluntary are likely to drive levels of trust that contribute to the optimisation of IS platforms for private sector institutions and to incentivise their participation.

We noted at the outset of this article that both NIS and IFC3 are in the early stages of their development and that additional *praxis* is necessary to draw firm conclusions about improving these IS models. In conclusion, we argue that practical experience not only needs to be garnered, but that it is critical to share the benefits and drawbacks of these IS platforms with a broader community of IS practitioners, regulators, and academics. Confidentiality is core to effective and reliable information sharing; yet to the extent that models, measures, and effective guidelines are, in their turn, shared – best practices for IS will emerge and have the potential to enhance cybersecurity across jurisdictions. Such best practices include automated protocols and tools for IS, a sharer option for anonymity with respect to other sharers, a high level of security and resilience for platforms, and inter-jurisdictional scaling up.

18 *See* an alternative view in Siboni and Klein (2016).

19 This may already be occurring within CERT-IL, although there is no mention of it in the *CERT Operating Principles*. *See* National Cyber Authority (n.d.). CERT Operating Principles, definition of "Cooperating entities".

20 The proposed government cybersecurity bill does address this issue (*supra* note 15).

Practical experience not only needs to be garnered, but that it is critical to share the benefits and drawbacks of these IS platforms with a broader community of IS practitioners, regulators, and academics.

Significant challenges lie ahead for IS to ensure that the information shared is consistently relevant, timely, and sufficiently detailed to bring real added value to sharers in the IS process – be they government or private sector actors. Moreover, as our understanding of hostile activity in cyberspace and its indicators expands, IS measures and capabilities will need to develop in tandem.

We conclude by noting two future challenges for IS platforms, as they become increasingly critical to cybersecurity. The first is the development of needed levels of their confidentiality and robustness, so that they may be leveraged for the responsible disclosure of vulnerabilities through IS (The White House, 2017; National Cyber Security Center, 2013; Herpig, 2018). Secondly, new measures are needed for the inclusion of stakeholders that bring new types of data and diverse perspectives to the IS platform, such as individual end-users of cyber products and services, while ensuring that trusted relationships among sharers and the added value of IS for all of them are maintained. ■

About the author:

Deborah Housen-Couriel, Adv.

Deborah Housen-Couriel's Tel Aviv-based law practice advises global and Israeli clients on strategies for regulatory planning and compliance in the areas of cybersecurity law and regulation. She teaches courses on cyber law at Hebrew University and at the Herzliya IDC and is a lead researcher at several Israeli universities. Deborah was a member of the Group of Experts that drafted Tallinn Manual 2.0; and currently serves as a Core Expert for the MILAMOS project and as Chair of a Working Group at the Global Forum on Cyber Expertise.

References

Antitrust Commissioner. (2017). Public Statement 3/17: *Information Sharing for Coping with Cyber Threats* (in Hebrew).

Bank of Israel. (2015). Directive 361, Cyber Defense Management. Art. 65 and 66.

Computers Law. (1995). Retrieved from: http://law.co.il/media/computer-law/computers_law_nevo.pdf (in Hebrew).

ENISA. (2016). Challenges for National CSIRTs in Europe 2016: Study on CSIRT Maturity.

ENISA. (2017). *Exploring the opportunities and limitations of current Threat Intelligence Platforms.* Retrieved from: https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms.

ENISA. (n.d.). CSIRTs by Country. Retrieved from: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.

ETSI. (2017). *Cyber: Implementation of the NIS Directive.* (DTR/CYBER-0021). p. 7. Retrieved from: https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf.

European Commission. (2013, February 7). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN 2013 final.

European Commission. (2016, July 5). Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final.

European Commission. (2018, May 4). State-of-play of the transposition of the NIS Directive. Retrieved from: https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive.

Government of Israel. (2011, August 7). Resolution 3611 (in Hebrew).

Government of Israel. (2015a). Resolution 2443 (in Hebrew).

Government of Israel. (2015b). Resolution 2444 (in Hebrew).

Government of Israel. (2018). Bill on Cybersecurity and the National Cyber Directorate (in Hebrew).

Haber, E. and Zarsky, T. (2017). Cybersecurity for Infrastructure: A Critical Analysis, *Florida State University Law Review*, 44(2).

Herpig, S. (2018). *Governmental Vulnerability Assessment and Management. Stiftung Neue Verantwortung.* Retrieved from: https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf.

Housen-Couriel, D. (2017). National Cyber Security Organization: Israel. *CCDCOE.*

Housen-Couriel, D. (2018). Information Sharing for the Mitigation of Hostile Activity in Cyberspace: Comparing two nascent models (Part 1). *European Cybersecurity Journal*, 4(3). pp. 44-50.

Katulić, T. (2018). Transposition of EU Network and Information Security Directive into National Law. *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).* p.1331. Retrieved from: http://docs.mipro-proceedings.com/iss/iss_03_4720.pdf

Law for Regulating Security in Public Bodies. (1998). Retrieved from: https://docs.google.com/viewer?url=http%3A%2F%2Fmain.knesset.gov.il%2FActivity%2Fcommittees%2FForeignAffairs%2FLegislationDocs%2Fsec7-2.doc (in Hebrew).

Ministerial Security Committee. (2002, December 11). Decision B/84.

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

Ministry of Finance. (n.d.). Cyber and Finance Continuity Center. Retrieved from: https://mof.gov.il/en/About/Units/CyberEmergenciesSafetyDraft/Pages/CyberCenterAndFinancialContinuity.aspx.

National Cyber Authority. (n.d.). CERT Operating Principles (in Hebrew).

National Cyber Security Centre. (2013). Responsible Disclosure Guideline. Retrieved from: https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html.

Robinson, N. and Disley, E. (2010). Incentives and Challenges for Information Sharing in the Context of Network and Information Security. *ENISA.*

Shtokhamer, L. (2018). *CERT Operation: Financial Case Study* (presentation).

Siboni, G. and Klein, H. (2016). Information-Sharing Challenges in an Intra-Sectorial Environment. *Military and Strategic Affairs*, 8(1), pp. 41-58.

Supervisor of Capital Markets. (2016). Circular on Management of Cyber Risk.

Supervisor of Capital Markets. (2018). Results of a Cyber Audit (in Hebrew).

Tabansky, L. and Ben Israel, I. (2015). *Cybersecurity in Israel.* Springer. pp. 31-34.

Weis, M. (2017, September 17). Presentation at the National Fintech Cyber Ecosystem Round Table (notes on file with author).

Weis, M. and Shtokhamer, L. (2017, June 25). *The Cyber and Finance Continuity Center* (presentation, in Hebrew).

The White House. (2017). Vulnerabilities Equities Policy and Process for the United States Government.