# Considerations for NATO in Reconciling Challenges to Shared Cyber Threat Intelligence: A study of Japan, the US and the UK

**Chon Abraham**
Associate Professor of Management Information Systems
William & Mary

**Sally Daultrey**
Chief Intelligence Analyst
Adenium Group

**Abstract:** Efforts for developing approaches to exchange information on security incidents, known as Cyber Threat Intelligence (CTI) sharing, are an international imperative for global cyber defence.  Japan, the US and the UK are the predominant allied entities in defence of maritime operations for global supply chains in the Asia-Pacific region. These states share common adversaries in cyberspace that work to weaken defences that NATO countries and partners seek to sustain.  This chapter explores the challenges and enablers for more effective CTI sharing between Japan, the US and the UK. This chapter offers insights for other non-NATO partners in collectively addressing the global menace of malicious cyber operations, strategic campaigns, and collateral damage on shared networks, infrastructure and missions.

**Keywords:** *Cyber threat intelligence, cyber security governance, information sharing*

## 1. Introduction

Cyber threats are fundamentally changing the nature of warfare and the digital economy with implications for international collaboration and security cooperation (NATO, 2019). Governments and the leadership of multinational companies must understand threat vectors and threat actors to activate their collective response, both in peacetime and during targeted cyber operations. Efforts for developing approaches to exchange information on security incidents, known as Cyber Threat Intelligence (CTI) sharing, is an international imperative (Menges et al., 2019) and governments can no longer rely on voluntary compliance across business ecosystems and supply chains to operationalise international cyber defence. Cyber operations are increasingly understood as linked to strategic campaigns, particularly when initiated by adversarial countries seeking to shift the relative balance of power amongst targeted countries with rippling global effects (Harknett and Smeets, 2020; NATO CCDCOE, 2017). CTI sharing is therefore essential for all directly and indirectly targeted societies and countries to build a collective understanding of these cyber operations and strategic campaigns in terms of: (1) their true nature; (2) the global reach of effects; (3) the duration; and (4) the extent of data exfiltration and aggregation compromising national security. The sophistication and proliferation of cyber threats are outpacing the capacities of countries to respond using conventional decision structures, to be replaced by dynamic bilateral and regional collaboration architectures. CTI sharing is vital to protecting the global business ecosystem and shared security interests, yet not all nations have comparable capabilities to effectively share and act on threat information.

Japan is NATO's longest-standing partner outside the Euro-Atlantic area and is particularly important to NATO's Asia-Pacific maritime operations (NATO, 2020). Understanding Japan's threat intelligence capabilities and challenges will help in understanding the capabilities of NATO allies like the United States (US) and United Kingdom (UK) in their roles as regular and established partners in maritime operations and trade relations. This chapter explores how more effective CTI sharing between Japan, the US and UK could be promoted, offering insights, which may serve other non-NATO partners in collectively addressing the global menace of malicious cyber operations, strategic campaigns and collateral damage on shared networks, infrastructure and missions.

As part of a larger research project sponsored by the Abe Fellow Program, we conducted 80 interviews over two years with government and private-sector personnel across Japan, the US and UK.[1] We also attended conferences and reviewed the literature on CTI sharing between and among the three countries, strategic culture, cyber risks to critical infrastructure and cyber corporate espionage.[2] In this analysis, we present one facet of the cooperation challenge—understanding the challenges to CTI–which our

[1] Data collection lasted over a two-year period from 2017 to 2019, consisting of insights gather from literature and interviews held face-to-face in-country or virtually that ranged 15 minutes to an hour using open-ended questions or allowing interviewees to provide narratives on the topic. Some insight was gathered from question and answer periods at conferences, meetings or other discussions. When permitted, sessions were recorded, translated, and transcribed. Thematic patterns were analysed in the data relevant to the challenges to CTI from technological, legal, or strategic cultural constraints that impeded seamless transfer of information across nations. Perspectives were sought from respective national cyber authorities, political leaders involved in cyber strategy development, private sector cyber security consultants to these national cyber entities and academic researchers involved in developing national capabilities for CTI. Interviews were conducted by Chon Abraham and Sally Daultrey. When a person who was interviewed required anonymity, in-text references omit interviewee's name. Information was obtained also by personal communication of the authors.

[2] See Appendix I for a summary of research methods.

research to date suggests is the most urgent task and greatest challenge in operationalising international collaboration. It is not enough to know that CTI can be supplied; partners need to know that information will be acted on when received. To reach this level of confidence requires, among other factors, understanding of CTI capabilities within the 'receiver' partner and an appreciation of strategic culture among those involved in the ecosystem of decision, action and accountability.

This chapter presents background literature augmented by insights from the interviews on collective responses and challenges for CTI. We then provide considerations for NATO partners and allies and offer concluding remarks that may guide future research on international CTI sharing.

## 2. Cyber Threat Intelligence Sharing: Research Context, Insights and Challenges

The WannaCry and NotPetya incidents of 2017, the effects of which can still be seen today, focused government attention on the scale of vulnerabilities in shared global supply chains and civilian infrastructure, particularly in cargo terminals and healthcare services. In May 2018, the European Parliament concluded that these events 'represent breaches of international law by, respectively, the Russian Federation and North Korea, and that the two countries should face commensurate and appropriate responses from the EU and NATO' (European Parliament, 2018). Calls for an international response (NATO CCDCOE, 2017) to the menace of global cyber threats placed cyberspace among the top five global risk domains for 2018 and 2019 (Economist Intelligence Unit, 2019; 2018). Cyber operations are increasingly understood as features of global campaigns (Harknett and Smeets, 2020; Smeets and Lin, 2019) and understanding the extent, tactics and timescale of these campaigns will benefit all who rely on cyberspace and can be significantly improved and accelerated if governments and multinational companies share CTI (114th US Congress, 2015). For example, the Japan-US Defence Cooperation guidelines have included cyberspace since 2015, stating that both governments will cooperate to protect critical infrastructure (Lewis, 2015). In the event of a cyber attack against any part of Japan's critical infrastructure, which is also used by the US Armed Forces and Japan Self-Defence Forces (JSDF), Japan will have the primary responsibility to respond with support from the US (Kyodo, 2019). This could escalate to the US conducting offensive operations on behalf of Japan, raising the stakes for both countries in their response to malicious cyber actors.

The lack of balanced capabilities for CTI fuels risks for vulnerabilities in collective responses for thwarting cyber attacks. For example, the 2013 framework of the US-Japan Defence Cooperation included an Information Security Agreement that allows for the exchange of classified information (US DOD, 2015; MOFA, 2005). However, according to interviewed cyber authorities, Japan still lacks direct access to a shared platform that can deliver forensic data for rapid attribution of cyber attacks. The imperative to address cyber security risk across national economies, legacy infrastructures and the defence industrial base is today recognised as a priority for national security strategy (Afina et al., 2020; Dunn Cavelty et al., 2019) and a fundamental activity of corporate governance in the digital age (Schinagl and Shahim, 2020). Cyber security has evolved from an enterprise wholly owned by information technology (IT) specialists (von Solms and von Solms, 2018; Naughton, 2016; von Solms and van Niekerk, 2013; Stevens, 2012; Hansen and Nissenbaum, 2009) to a whole-nation challenge that requires active collaboration, set against the human challenges of organisational change, governance and strategic culture. We explore how these challenges have affected the capacity for Japan to share and act on threat intelligence and build effective cyber defence collaboration with the UK and the US that may have implications for other partner and allied NATO countries.

## 3. CHALLENGES TO SHARING CYBER THREAT INTELLIGENCE

Countries vary in their definition of cyber security but nearly all have drafted some form of cyber security strategy[3] within the past decade, with national cyber security strategies typically developing as part of a coordinated review of national security strategy (Baezner and Cordey, 2019; Luiijf et al., 2013). NATO allies broadly agree on the need to increase cyber resilience, build capabilities including in information sharing and facilitate international collaboration (Ablon et al., 2019; Pernik, 2014), while the imperative for CTI sharing as an organisational capability rather than a data-set is widely recognised in the professional global cyber security community (Wagner et al., 2019). Research in the past decade has begun to compare national cyber strategies for evidence of governance modes (Shackelford and Kastelic, 2015; Weiss and Jankauskas, 2019), harmonisation (Kolini and Janczewski, 2017; Štitilis et al., 2017) and membership of international organisations (Kolini and Janczewski, 2017). Limiting factors and barriers to cooperation in global cyber defence that we have identified include: (i) the capacity and willingness to share threat intelligence; (ii) fuzzy boundaries of responsibility and accountability; and (iii) incomplete or inaccurate understanding of partners' expectations and strategic culture.

*A. Challenge One: Capacity and Willingness to Share Threat Intelligence*
The US and Japan identified barriers to rapid information-sharing as a particularly complex operational challenge in activating international cooperation for CTI. Incompatible platforms, legal and jurisdictional constraints and conflicting or incompatible strategic cultures were all described as limiting factors. These issues have similarly been identified in studies of CTI-sharing among companies (Wagner et al., 2019; Menges et al., 2019; Koepke, 2017) and for NATO, where inter-organisational trust, incompatible platforms and time-lag in sharing information are among the seven challenges which limit NATO's capacity to work seamlessly with multiple partners (Tolga, 2019). NATO currently uses the Malware

[3] See the NATO CCDCOE library for an index of national cyber strategies (NATO CCDCOE, 2020).

Information Sharing Project (MISP) and launched a Cyber Security Collaboration Network in February 2019 (Pernik, 2014).[4] Japan has formal collaboration agreements with the US and U amongst others, but technical ability for day-to-day collaboration is limited as Japan does not have an interoperable, point-to-point threat intelligence platform allowing direct receipt of data. This is particularly problematic for classified data associated with CTI. Accepted CTI protocols within the threat intelligence community include Structured Threat Information Expression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII). These are standards that the US-CERT Automated Indicator Sharing (AIS) capability uses for CTI in the private sector. While senior cyber security researchers and personnel within Japan's cyber authorities have not explicitly noted the use of NATO's adopted MISP, they have observed that some Japanese agencies use STIX as a standard and AIS to share some CTI with US-CERT. However, there is not consistent use across all agencies and in private-public engagements.

We contextualise our analysis of national posture and strategy based on the premise that 'we need to get better at sharing what we know, faster'. The requirement for human interpretation of threat information means that automated CTI is not a fix-all (Wagner et al., 2019) and so the ideal–cyber defence at network speed–is likely to remain an unrealised goal in international cooperative cyber defence until collaboration architectures are stabilised on a foundation of inter-organisational and cross-cultural trust and standardised CTI terminology. Nations need the ability to see a threat and then talk about it on equal terms and this needs direct connectivity for timely response and attribution. According to intelligence personnel that were interviewed in the US, Japan is not getting the full picture fast enough, particularly for classified information that involves CTI (Abraham's interviews and pers. comm., 2019 2 December). This is in part because Japan's cyber personnel in, for example, the Ministry of Defence (MOD), connect with their international peers via proxies, sometimes in allied countries. The process requires de-aggregation and declassification of data for transit and then reassembling when received into classified information sources.

Our interviews also noted a lack of the skill and acumen necessary to understand how to synthesise multi-source threat intelligence in Japan's self-defence forces (JSDF) and other public cyber authorities (Abraham's interviews and pers. comm.,18 December 2019). While the MOD does have something that resembles a cyber-focused speciality akin to those of the US and UK, JSDF cyber personnel are sanctioned to only protect MOD critical infrastructure, even if cyber attacks are detrimental to the Japanese government or society as a whole (Gady and Koshino, 2020). Article 76 of the Self-Defense Forces Act does not define cyber attacks as armed attacks allowing the use of JSDF (Gady and Koshino, 2020; Kono, 2015).[5] This has implications for how the JSDF can cooperate domestically to build cyber acumen in the public and private sectors

[4] See more information provided by the NATO Communications and Information Agency and the MISP (NCIA, 2018; MISP, 2020.)

[5] For a detailed discussion of how cyber attacks are defined in Japanese law, see (Kono, 2015).

and internationally, such as participating in joint cyber offensive training. Deep learning, particularly regarding threat hunting, forecasting intrusion methods, collecting and analysing signal intelligence and forensics on cyber data and networks to determine attribution, are skills needed in Japan's cyber workforce (Abe, 2020). For example, the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) is designated as Japan's cyber coordinating authority, yet operates under a constrained budget and does not have equal legal authority with other agencies and ministries. This reduces its effectiveness and workforce development as it relies on personnel assigned from other Japanese government agencies or the private sector (with or without cyber background), who are rotated in and out of the organisation. The NISC is also constrained in its ability to enforce cyber policy, which is currently fragmented across various ministries. This further limits its ability to influence how Japan's cyber workforce is developed, maintained and provisioned to access and use CTI and related data of various security classifications.

Another practical and major constraint to effective collaboration is Japan's lack of a comparable personnel security clearance system and management programme to ensure classified data is properly handled. Partners need to know that shared intelligence is used and handled safely. These problems are compounded by ambiguity in its classified data ontology to appropriately tag data in compliance with other NATO member countries and partners. There is a disparity in how Japan classifies threat intelligence data in comparison to the US and UK, but consistency is required for nations to be responsive in assessing the effects of threats and their analysis and in timely attribution. According to our interviews, this is also the basis for the difficulty in sharing CTI internally across government and cyber agencies and the private sector. (Abraham's interviews and pers. comm., 2019 4 March, 2 December, 18 December).

While Information Sharing and Analysis Centres (ISACs) are increasingly being used across critical national infrastructure (CNI) sectors in Japan to more quickly readily threat warnings, alerts of malicious activities and threat mitigation data, the detailed classified data required for attribution is often delayed, sometimes by days. US Department of Defense (US DOD) and Japan's Ministry of Defense are exploring options for resolving this issue that are primarily military-to-military, and collaborative exercises for enhancing joint cyber operations and threat intelligence sharing with public entities in the Ministry's cyber task forces and vendors in CNI sectors. The Cybersecurity and Infrastructure Security Agency (CISA) is advising Japan on how to organise an approach around identifying critical national functions that can home in on critical threats to investigate and more effectively coordinate responses. However, this again requires a platform for domestic information exchange. Japan recognises the requirement to be more accountable as a partner to NATO member countries and is actively taking steps to address deficiencies in its capacity to cooperate with others. On 14 August 2020, Defence Minister Taro Kono announced that Japan would seek to expand links with the Five Eyes intelligence-sharing alliance, as this would allow Japan to obtain classified information at an earlier stage in threat assessment and response (Abe and Rieko, 2020).

As Japan considers the use of offensive cyber capabilities, alliances with NATO and other partners will need a minimum understanding of what tools and weapons have been validated and transparency about at least the function of these cyber assets. Cataloguing and evaluating capacities and cyber assets across countries will help with rapidly mobilising threat intelligence sharing efforts in joint cyber efforts and allowing ease of universal deployment of security standards and vetted state-of-the-art tools. Japan also needs increased capability in assessing how secure the infrastructure is for data transmission and what Japan is equipped to do in terms of technology and personnel skills in the event of a cyber incident at national or international level. According to sources interviewed for this research, a model for assessing this maturity employed by the US Office of the Director of National Intelligence (ODNI) and US Department of Defense is being proposed to the Government of Japan (Abraham's interviews and pers. comm., 6 June 2019).

Limited capacity to absorb and act on CTI compounded by differences in classification and uncertainty over how CTI may be shared, creates a barrier to building trust among partner nations. Continuously improving collective ability to provide threat intelligence and act on it will build capacity to achieve attribution in a timescale that is meaningful for defence and prosecution. This can only be achieved through a whole-of-nation approach.

### *B. Challenge Two: Boundaries of Responsibility and Accountability*

Much of the global attack surface is owned and controlled by the private sector (Ablon et al., 2019; Baezner and Cordey, 2019; Abraham's interviews and pers. comm., 2019 6 June, 8 August, 10 December). Therefore, national cyber security by definition requires cooperation by government organisations with the private sector, within and across national boundaries. Most malicious cyber activity, whether it is cybercrime or potentially of national security importance, happens on privately owned networks. Those private networks are typically not transparent to government cyber authorities in NATO countries. The US, UK and Japan have mechanisms for the private sector to engage and share information, but the robustness of this capacity differs, as does the trust level between the private and public sectors that threatens cyber authorities' ability to receive timely information or to provide assistance. While there are technologies to assist policing entities to determine malicious cyber activity when personal devices such as smartphones are involved (Weaver, 2020; Chesney, 2017), permission for authorities to access private organisational networks is a different matter.

In the opinion of personnel interviewed in the US and UK, the ideal solution for gathering and building CTI for sharing and attribution post-intrusion is to have proper weblogs and backups (Abraham and Daultrey's interviews and pers. comm., 2019 14 July and 9 August; R. Wainwright, 2018, conference and pers. comm, 12 December). With weblogs, authorities can conduct full forensic analysis which allows law enforcement to conduct two primary functions: use their legal authority and powers to obtain data from other media beyond the initial victim such as infrastructure platform service providers and collate victim web log information with other data points obtained through legal authorities to reconstruct the intrusion and learn about the adversary's tactics. Law enforcement personnel in Japan, the US and UK note that it can be difficult to obtain permission to access private networks, even if there is a suspicion of malicious cyber activity by the private-sector victim organisation (NEC, 2017). In Japan, companies are even less likely to invite government cyber authorities in to aid in determining facts of the intrusion, data exfiltration and insights for remediation. This is due to fear of reputational harm if it is revealed publicly that the company has suffered a cyber attack and was thus not a good steward of its customers' data. CTI is thus limited by transparency and trust within the private sector (NEC, 2017).

Incentivising and activating the private sector to participate in national cyber defence and be held accountable by incorporating robust threat intelligence capabilities into cyber security practice was identified by all interviewees as both a problem and an opportunity (Abraham and Daultrey's interviews and pers. comm., 2019 14 July and 9 August; R. Toth, 2019, pers. comm., 2019 21 July; M. Tsuchiya, M. McConnell, M. Chida, M. Otaka, 2018, conference and pers. comm., 2019 12 December). Companies in Japan have been slow to adapt: only about half conduct cyber security risk assessments that would include their capability to receive and digest threat intelligence data, compared with about 80 per cent in the US and 65 per cent in Europe (Matsubara, 2018b). The lack of cyber leadership in Japanese companies may account for this deficit, as only 27 per cent employ a Chief Information Security Officer (Matsubara, 2018b). Applying risk management standards such as using the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) and creating trusted vendor pools of non-blacklisted entities, especially for the defence industrial base, that are also required to share and act on threat intelligence, can all contribute to building a robust threat-sharing public/private ecosystem (Feldman and Witte, 2017).

However, in Japan, cyber and police officials note reluctance by government to receive and relay information to the private sector regarding companies or any entity blacklisted in other nations for dubious behaviour in cyberspace, such as those on the US Department of Treasury Office of Foreign Assets Control (OFAC) list that operationalises cyber protections in the US Foreign Investment Risk Review Modernisation Act. This reluctance stems from fear of both disadvantaging a company if that intelligence is not valid, or infringing its autonomy to manage its internal business processes. This promotes a lack of transparency for cyber events of national security interest and loss of potentially vital threat intelligence data—some of which may date back many years—by Japanese defence contractors. The problem is exacerbated beyond Japan because these contractors also supply other nations, including the US, UK and other NATO countries. In Japan, there is typically no naming, shaming or fines for companies that do not act on threat intelligence even when shared, which contributes to a frail CTI-sharing domestic culture. This difference in business culture around threat perception and handling may have international implications, particularly for NATO. The Japanese House of Councillors is pushing for legislation requiring Japanese companies to disclose their cyber security postures on their financial statements, which would include their ability to process threat intelligence data. Other countries, including the US and UK, might consider this to encourage CTI capability adoption and cyber resiliency. Japanese companies' corporate taxes are reduced if they can prove that their IT investments include cyber security measures, including CTI processing infrastructure and the promotion of this capability for the shared benefit of the domestic public and private sectors and international stakeholders (M. Tsuchiya, 2019, pers. comm., 6 December; M. DePalo, 2019, pers. comm, 5 March; Matsubara, 2018a).

Globally accessible technologies employed by the private sector complicate CTI assessment for authorities. For example, global virtual private server (VPS) infrastructure can be leased by any private or public entity if allowed in the country. Hostile actors use this medium in cyber attacks, leasing VPSs for short periods, or weaponise leased media by other private sector entities. For law enforcement, getting access to data on VPSs is difficult if the data is in other countries. If the infrastructure is domestic, at least in the US there is a legal process for acquiring it. The Federal Bureau of Investigation (FBI) and Department of Justice (DOJ) have a legal process for gathering information via telecoms devices in the Communications Assistance for Law Enforcement Act (CALEA). However, VPSs are not yet regulated to enable threat intelligence for law enforcement; similarly, no such legislation yet exists in Japan or the UK. Here may be a role for NATO, as a non-state entity, to encourage collaboration for agreements instead of laws across international boundaries to enable threat intelligence gathering and sharing.

Adoption of robust threat intelligence practice and investment in capabilities is not internationally comparable. By 2018, most countries had enacted some form of cyber security legislation, but laws and sanctions are of limited effect against adversaries that do not recognise them (Intelligence and Security Committee of Parliament, 2020; Clarke and Knake, 2020; Stevens, 2012; Tsuchiya, 2019) in jurisdictions where the ability to enforce them is weak and attribution–which relies on threat intelligence – and prosecutions take months or years. A full comparative analysis of the legal basis for cooperation is outside the scope of this chapter, but we note that countries are limited by their own constitution, laws and agreements and the technical capacity to exercise authority within the boundaries of the law (Kono, 2015). For example, the JSDF is planning to develop offensive cyber capabilities that will require revisions to Japan's Self-Defence Forces Law to clarify actions that constitute retaliatory offensive actions (Gady and Koshino, 2020). This requires attribution and sophisticated threat analysis capabilities.

Organising and regulating collective cyber defence presents challenges for many governments and can thwart robust threat intelligence. While the concept of sovereign state security is fairly stable (Hansen and Nissenbaum, 2009), cyberspace uniquely challenges how sovereign countries organise and project political authority (Weiss and Jankauskas, 2019). In non-authoritarian regimes such as those of NATO allies and partner countries, the role of the state as a security guarantor, legislator, regulator and security partner is challenged by the realities of delivering cyber defence (Dunn Cavelty et al., 2019). Boundaries of responsibility (and thus accountability) are unclear (Stevens, 2012). This problem is illustrated sharply in the case of CNI, given that militaries typically rely partly on national infrastructure owned and operated by private sector organisations. The task of securing CNI from cyber attack has gained attention by governments in articulating their cyber security strategy, particularly after the cyber attacks on Ukraine's electricity grid in December of 2015 and 2016. The demarcation of cyber risk responsibility between utility owner and state is problematic and far from uniform. For example, Japan sees an equal division of labour between government and the private sector (Government of Japan, 2017), while the UK prefers that the private sector assumes responsibility. Coercion by threat actors using CNI and supply-chain vulnerabilities tests the capabilities of countries to respond. Cyber infiltration by adversaries operating within or for other countries seeking to gain intellectual property from US and Japanese defence contractors operating in the Asia Pacific over private networks illustrates the intertwined threats and potential collateral damage of allied and partner countries (MOD, 2018; Lewis, 2015; Tabuchi, 2011). In securing supply chains and shared networks, countries should require accountability by all parties to safeguard and share threat information to avoid proliferating effects.

Assigning responsibility and accountability implies structures and laws. Yet in cyber, analysis of roles and hierarchical structures is only the starting point for identifying barriers to cooperation in an apparently unified global threat landscape (Kuerbis and Badiei, 2017). In creating structures and governance tools, non-authoritarian governments in free-market economies face a challenge and a choice: to develop a single agency that 'owns' cyber on behalf of the nation (and supply a talent base to support it) or require all actors to adhere to laws and standards. The challenge with the first method is to develop a sustainable model that has the endorsement of the private sector while reconciling different organisational cultures (Hannigan, 2019). The second requires devising incentives and fines that are enforceable and adequate to the scale of the task. In a study of 100 cyber strategies and policies, Weiss and Jankauskas (2019) identified two governance modes: delegation and orchestration. When responding to threats, governments tend to delegate authority while maintaining hierarchical control, while in risk mitigation, governments use and orchestrate intermediaries. Overall, we recognise the delegation model in the UK, orchestration in Japan and a hybrid of the two in the US. Interviews for this research suggest that, in the case of the Japan Computer Emergency Response Team (JPCERT), currently a quasi-government entity, this could be formalised within government for delegation and orchestration of cyber security authority that would encompass the development of robust CTI capabilities to include technology, structural governance and processes and skills enhancement (L. Wells, 2019, pers. comm., 15 June; N. Jones, 2019, pers. comm., 12 June; N. Toshio, 2018, pers. comm., 3 September).

The chief cyber security strategist at a leading Japanese corporation observed that Japan has a unique challenge in that its employment system and intelligence community workforce development differ completely from those in the US and the UK. Japan still largely depends on a lifetime employment system in which an employee will start with a company and remain there until they retire. As a result, cyber security experts that have cut their teeth in the Japanese government or intelligence communities rarely move to the private sector or vice versa. JPCERT, as an established organisation for incident response, and NISC, established as the coordinating authority for cyber policy, have fewer resources than ministries in their budget for workforce development that affects the continuity of operations and knowledge management in cyber security (K. Fujisue, 2020, pers. comm., 7 March; N. Toshio, 2018, pers. comm., 3 September). Japan's challenges in resolving continuity and knowledge management issues are readily compared with the UK experience of setting up the National Cyber Security Centre (NCSC) in reconciling government and private sector organisational cultures (Hannigan, 2019). While more mature, the US cyber authority responsibility and accountability structure has sought through its maturation to define the lines between interested government entities and raise cyber acumen, particularly in threat hunting which is a preoccupying theme of the US Cyberspace Solarium Commission in its recommendations for strengthening US cyber defence (King and Gallagher, 2020). US and UK cyber and intelligence professionals and government officials have noted the need to have allies and partners like Japan that have comparable workforce cyber skills sets to maximise joint efforts, particularly in threat hunting and intelligence analysis. Therefore, there are efforts across military entities in the US, UK and Japan to equalise cyber acumen. While noting that no two organisations (or nations) handle cyber threats in the same way, workforce structures have a role in robust national threat intelligence capabilities. NATO may have a role here as a 'boundary entity' (Wagner et al, 2019) in defining a 'common operating language' and activating the global cyber defence knowledge ecosystem toward more effective CTI sharing.

### *C. Challenge Three: Understanding each other*

Dunn Cavelty and Egloff (2019, pg. 41) explain 'cybersecurity governance' as 'a risk management approach based on continuous monitoring, measurement and control [...seeking to] establish trust and stability of expectations among different actors' as originally defined by Bowen et al. (2006). The key phrase here is 'stability of expectations'. For threat intelligence shay ring, this means knowing that information exchanged will be safeguarded and acted upon in a timeframe useful for attribution. It is unrealistic–and perhaps unnecessary (Stevens, 2017)–to expect countries to adopt parallel structures, legislation and authorities. It is practically useful to the urgent task at hand for partners to agree on metrics and standards by which cyber security risk is minimised: in other words, 'we don't really mind how you do it, we just want to know that it has been done in a way that our systems and organisation can understand and engage with, at the moment when we need to work together'. Creating this common operating language based around a requirement to act on threat information may facilitate the rapid exchange of expertise and threat intelligence.

The obligations, permissions and preferences of countries collectively shape their global relations (Stevens, 2012), organisational cultures and national strategic culture. Strategic culture is strongly influenced by context: no state (or company) forms a cyber defence posture in isolation; experience of past success and failures contributes to shaping policy and actions. NATO's approach to cyber is rooted in the experience of adaptation to the security environment of the 1990s, cyber attacks on NATO operations in 1999 and security alliances of the post-9/11 era (Burton, 2015; Healey and Jordan, 2014). This same mindset applies today in building an approach to yet another challenge in the international security environment. In building and projecting a cyber defence posture, countries are influenced by world events, institutional memory and geopolitical imagination. US doctrine on information warfare emerged in the wake of Operation Desert Storm (Stevens, 2012) and the cyber attacks of 2006, while the cyber security political imagination of the US has been shaped by events such as Stuxnet (Stevens, 2018), the Office of Personnel Management (OPM) breach and the indictment of APT10. For Japan, 'year zero' was the 2011 attacks on Mitsubishi Heavy Industries (Kallender 2014), echoed in another attack on Mitsubishi in May 2020 (CSIS, 2020). In 2011, Japan's Ministry of Economy, Trade and Industry (METI) reported nearly 37 per cent of Advanced Persistent Threats (APTs) were focused on Japan's infrastructure, notably industrial control systems in power plants and manufacturing facilities (Kallender 2014). The UK is preoccupied with countering financial crimes and containing the cyber threat from Russia. These experiences collectively shape how Japan, the UK and the US approach the task of threat intelligence collection and sharing.

The US hopes that encouraging acceptable international behaviours in cyberspace will be more consistent with a shift in paradigm from mere deterrence to persistent engagement for seizing and gaining the operational advantage by actively engaging and contesting cyber behaviour by adversaries (Lopez, 2019; Miller and Pollard, 2019; Harknett, 2018). In seeking to 'remake cyberspace in its own image' (Segal, 2018: p. 10) through overseas investment in infrastructure and influence in international standards, China also effectively delivers a deterrent effect (Economist Intelligence Unit, 2017). Japan's entire approach to cyber security is limited by its pacifist constitution (Matsubara, 2018a) which contributes to hesitation in cyber attack attribution that is thought to potentially provoke retaliation or escalation to war (Nakasone, 2020). The UK's tendency to debate but then largely disregard parliamentary committee review outcomes across successive parliaments has the potential to render new legislation of little effect against embedded and persistent adversaries (Clarke and Knake, 2020; Intelligence and Security Committee of Parliament, 2020). Nations do not always act alike in response to the same threat (Ferguson, 2011; Stone, 2005), so understanding a partner's strategic culture can significantly improve the chances of success in joint working arrangements: indeed, one outcome of our interviews and research to date has been a modest contribution to understanding how our partners and allies think. Ablon et al. (2019) in their study for RAND have suggested that establishing a standardised Indications and Warning (I&W) model across NATO allies and partners should be a priority for nations to ensure their effective military presence in cyberspace. Building a 'common operating language' for threat intelligence sharing should include identifying where strategic cultures converge (and where they do not) because this helps in defining a minimum viable architecture for collaboration. This complexity in the translation of classification from sender to receiver further adds to the lag time in synthesising critical information to counter cyber threats and actual attacks—the cyber equivalent of having to pull out a dictionary in the middle of a live conflict. These deficiencies and incompatibilities prolong and complicate attribution and assessment of if and how domestic infrastructures were used or weaponised by an adversary.

The recent development in the US approach to CNI protection is key in re-evaluating how we conceptualise accountability, cyber risk and resilience because it considers capabilities across sectors and national critical functions, rather than stove-piping within industries. This approach finds ready comparison with the founding principles of NATO: while the Treaty does not name any specific threat or adversary, it does establish the 'operating principles for a defensive alliance' (Olsen, 2020, p. 5), which have not needed modification despite the growth of the Alliance to include a much more diverse membership than at its inception. The UK is also moving toward consideration of critical systems (akin to functions) and assessing their vulnerability to cascading risks,[6] a practice generally less formalised in government but vital for characterising the environment in which threat intelligence must perform (Wells et al., 2017). Identifying a 'common operating language' for threat intelligence sharing, including identifying and aligning where strategic culture and governance tools converge (and where they do not) can help to define a minimum viable architecture for international collaboration.

## 4. CONSIDERATIONS FOR NATO

Reviewing collaboration agreements between the UK, Japan and the US since 2008 we find an emphasis on action outstanding. In particular, the experiences of Japan illustrate that domestic infrastructure must be in place to effectively enable CTI sharing among internal government and private sector entities that can be leveraged for external communication to allied and partner nations. Even though the technologies exist in Japan to support more robust CTI, strategic culture plays a role in constraining how, where and by whom intelligence can be shared and acted upon. For example, some constraints stem from privacy and trust issues between the public and private sector, how expertise in work is traditionally developed impacting cyber skillset development, and fears associated with potential retaliation from active attribution or offensive cyber operations. Domestic laws can also constrain

[6] See e.g. CRUISSE Project, a research consortium with the National Security Secretariat of the UK Cabinet Office (NSS, UK Cabinet Office, 2019).

capability developments particularly those that do not provide needed cyber security legal authority to those government entities that establish policy, which also undercuts funding for cyber authorities and limits capability for workforce development. Insights from Japan's experiences in adapting to global cyber threats suggests an imperative to understand these differences across nations and seek methods to overcome these barriers.

While the requirement for multinational cyber cooperation is challenged by unbalanced technical capabilities, strategic cultures and legal frameworks, NATO is well-positioned to enable partner and allied nations to share CTI, particularly by assisting with enabling use of its MISP and encouraging best practice in provisioning cyber authority structures for threat intelligence sharing as part of a potential international cyber security maturity, resilience development and assessment programme. For this programme, the NATO Cooperative Cyber Defence Centre of Excellence could take the lead in:

> (1) reconciling incompatibilities and promoting level setting of threat intelligence capabilities across partner and allied nations to speed the flow of information;
>
> (2) coordinating agreements to ensure trusted threat intelligence information is acted upon;
>
> (3) enabling partners and allied countries to adopt a minimal set of classification standards, compatible ontologies and comparable personnel security clearances management programs that enable threat intelligence sharing;
>
> (4) encouraging the development of a threat intelligence maturity scale that addresses technology, process, and workforce capabilities to aid nations in readily identifying specific improvements to benefit the international threat intelligence ecosystem; and
>
> (5) developing mechanisms to promote accountability in global industries to build threat intelligence capacity and trusted sharing with public entities for the international cyber mission.

Making CTI sharing viable requires that partner nations start talking the same language and allow for some compromise on blaming, naming and shaming, to encourage the private sector to take more responsibility and contribute to the national cyber mission of their respective governments. Implications for NATO partnerships include identifying structures and practices among partners that are not constrained by strategic culture and exploring the scope for NATO's role—as a non-state actor—in defining a 'common operating language' for CTI architectures and practices. Building comparable threat intelligence capabilities under the constraints we have identified in this study is extremely difficult. Yet, the requirement to accelerate and facilitate effective global cooperation in cyber defence is urgent. Thus, in undertaking this charge NATO can truly be unfettered in deliberation to thwart the ability of any entity to weaponise the cyberspace domain.

## 5. ACKNOWLEDGEMENTS

This chapter presents selected insights from research conducted over two years, supported in part by the Abe Fellows Programme and the US Social Sciences Research Council. The authors gratefully acknowledge the perspectives given by cyber security practitioners and officials in the US, Japan and the UK. The views are the authors' own interpretations and do not represent the official positions of Japan, the US, UK or organisations with whom we are affiliated or engaged with during this study.

## 6. REFERENCES

Abe, D. (2020) 'Lagging China and the US, Japan to Beef up Cyber Defense'. *NikkeiAsia.* Available at: https://asia.nikkei.com/Politics/Lagging-China-and-the-US-Japan-to-beef-up-cyberdefense [Accessed: 30th September 2020].

Abe, D. and Rieko, M. (2020) 'Defense Minister Taro Kono speaks during an interview on Aug. 12 in Tokyo'. *NikkeiAsia*. Available at: https://asia.nikkei.com/Editor-s-Picks/Interview/Japan-wants-de-facto-Six-Eyes-intelligence-status-defense-chief

Ablon, L. et al. (2019) *Operationalising Cyberspace as a Military Domain: Lessons for NATO*. RAND Corporation. Available at: https://www.rand.org/pubs/perspectives/PE329.html [Accessed: 13th August 2020].

Afina, Y., Inverarity, C. and Unal, B. (2020) *Ensuring Cyber Resilience in NATO's Command, Control and Communication Systems*. London: Royal Institute of International Affairs. Available at: https://www.chathamhouse.org/publication/cyber-resilience-nato-command-control-communication-afina-inverarity-unal.

Baezner, M. and Cordey, S. (2019) *National Cyber security Strategies in Comparison – Challenges for Switzerland*. Zurich: Center for Security Studies (CSS), ETH Zürich.

Bowen, P., Hash, J. and Wilson, M. (2006) *Special Publication 800-100. Information Security Handbook: A Guide for Managers* (Gaithersburg: National Institute of Standards and Technology (NIST), 2006), p.6.

Burton, J. (2015) 'NATO's cyber defence: strategic challenges and institutional adaptation'. *Defence Studies*. 15(4), pp. 297–319.

Center for Strategic Information Studies (2020) 'CSIS Significant Cyber Incidents'. *CSIS website*. Available at: https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents [Accessed: 24 July 2020].

Chesney, R. (2016) 'A Primer on Apple's Brief in the San Bernadino iPhone Fight'. *Lawfare.* Available at: https://www.lawfareblog.com/primer-apples-brief-san-bernadino-iphone-fight [Accessed: 26th September 2020].

Clarke, R. A. and Knake, R. K. (2020) *The Fifth Domain*. New York: Penguin Random House.

Dunn Cavelty, M. and Egloff, F. J. (2019) 'The Politics of Cybersecurity: Balancing Different Roles of the State'. *St Antony's International Review*. 15(1), pp. 37–57.

Economist Intelligence Unit (2017) *China Going Global*. London. Available at: https://www.eiu.com/public/topical_report.aspx?campaignid=ChinaGoingGlobal [Accessed: 13th August 2020].

Economist Intelligence Unit (2018) *World risk: Alert – Global risk scenarios*, *Risk Briefing*. London. Available at: http://viewswire.eiu.com/index.asp?layout=RKArticleVW3&article_id=1876319171 [Accessed: 8th August 2020].

Economist Intelligence Unit (2019) *Cause for concern? The top 10 risks to the global economy 2019*. London. Available at: https://pages.eiu.com/rs/753-RIQ-438/images/Global_risks_2019.pdf [Accessed: 8th August 2020].

European Parliament (2018) 'Report on Cyber Defence'. Available at: https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_EN.html [Accessed: 8th August 2020].

Feldman, L. and G. Witte (2017) 'Cyber threat intelligence and information sharing'. National Institute of Standards Information Technology Labs Bulletin. Available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=923332 [Accessed: 25th September 2020].

Ferguson, J. (2011) 'The U.S.-Japan Alliance and Russia', in Inoguchi, T., Ikenberry, G. J., and Sato, Y. (eds) *The U.S.-Japan Security Alliance*. New York: Palgrave Macmillan US, pp. 195–216.

Gady, F. and Y. Koshino (2020) 'Japan and cyber capabilities: how much is enough?'. Available at: https://www.iiss.org/blogs/military-balance/2020/08/japan-cyber-capabilities [Accessed: 25th September 2020].

Government of Japan (2017) 'The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)'. Available at: http://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf [Accessed: 13th August 2020].

Hannigan, R. (2019) 'Organising a Government for Cyber'. *Royal United Services Institute for Defence and Security Studies*. Available at: https://rusi.org/sites/default/files/20190227_hannigan_final_web.pdf [Accessed: 24th July 2020].

Hansen, L. and Nissenbaum, H. (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School'. *International Studies Quarterly*. 53(4), pp. 1155–1175.

Harknett, R. (2018) 'United States Cyber Command's New Vision: What It Entails and Why It Matters,' Lawfare. Available at: https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters [Accessed: 26th September 2020].

Harknett, R. and Smeets, M. (2020) 'Cyber campaigns and strategic outcomes'. *Journal of Strategic Studies*. March 2020, pp.1-34.

Healey, J. and Jordan, K.T. (2014) 'NATO's Cyber Capabilities: Yesterday, today, and tomorrow'. Issue Brief, September 2014, Atlantic Council.

Intelligence and Security Committee of Parliament (2020) *Russia*. HC632. London: UK Government.

Kallender, P. (2014) 'Japan, the Ministry of Defense and Cyber-Security: Progress and Pitfalls'. *The RUSI Journal*. 159(1), pp. 94–103.

King, A. and Gallagher, M. (2020) 'US Cyberspace Solarium Commission Report'. *US Cyber Solarium Commission website*. Available at: https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view [Accessed: 24th July 2020].

Kolini, F. and Janczewski, L. (2017) 'Clustering and Topic Modelling: A New Approach for Analysis of National Cybersecurity Strategies'. *PACIS 2017 Proceedings*. Available at: https://aisel.aisnet.org/pacis2017/126 [Accessed: 24th July 2020].

Kono, K. (2015), 'A Japanese Perspective on Deterrence in Cyberspace Grey Zone Contingencies and the Role of the Japan-U.S. Alliance' in W. Harold, S. *et al.* (2015) 'The U.S.-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains'. Rand Corporation: Santa Monica.

Koepke, P. (2017), 'Cybersecurity information sharing incentives and barriers'. CISL Working Paper 2017-13. MIT Sloan School of Management.

Kuerbis, B. and Badiei, F. (2017) 'Mapping the cybersecurity institutional landscape'. *Digital Policy, Regulation and Governance*. 19(6), pp. 466–492.

Kyodo, J. (2019) 'U.S. to defend Japan from cyberattack under security pact'. *Japan Times*. Available at: https://www.japantimes.co.jp/news/2019/04/20/national/politics-diplomacy/first-japan-u-s-say-security-treaty-cover-cyberattacks/ [Accessed: 24th July 2020].

Lewis, J. (2015) 'U.S.-Japan Cooperation in Cybersecurity'. CSIS publication. Available at: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151105_Lewis_USJapanCyber_Web.pdf [Accessed: 23rd July 2020].

Lopez, T. (2019) 'Persistent Engagement, Partnerships, Top CYBERCOM's Priorities,' US DOD https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/ [Accessed: 24th July 2020].

Luiijf, E., Besseling, K. and Graaf, P. D. (2013) 'Nineteen national cyber security strategies'. *International Journal of Critical Infrastructures*. 9(1/2), p. 3.

Malware Information Sharing Program (MISP) (2020) 'MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing'. *MISP Threat Sharing website*. Available at: https://www.misp-project.org/index.html [Accessed: 24 July 2020].

Matsubara, M. (2018a) 'How Japan's New Cybersecurity Strategy Will Bring the Country Up to Par with the Rest of the World'. *Council on Foreign Relations*. Available at: https://www.cfr.org/blog/how-japans-new-cyber security-strategy-will-bring-country-par-rest-world [Accessed: 13th August 2020].

Matsubara, M. (2018b) 'How Japan's Pacifist Constitution Shapes Its Approach to Cyberspace'. *Council on Foreign Relations*. Available at: https://www.cfr.org/blog/how-japans-pacifist-constitution-shapes-its-approach-cyberspace [Accessed: 13 August 2020].

Miller, J. and N. Pollard (2019) 'Persistent Engagement, Agreed Competition and Deterrence in Cyberspace'. *Lawfare*. Available at: https://www.lawfareblog.com/persistent-engagement-agreed-competition-and-deterrence-cyberspace [Accessed: 26th September 2020].

Ministry of Defense (MOD) (2018) 'Security Surrounding Japan: Section 5 Trends in Cyberspace'. Available at: https://www.mod.go.jp/e/publ/w_paper/pdf/2018/DOJ2018_1-3-5_web.pdf [Accessed: 30 September 2020].

Nakasone, Y. (2020) *Japan – A State Strategy for the Twenty-First Century*. 1st edn. London: Routledge. Doi: 10.4324/9781315029467.

National Security Secretariat (NSS) UK Cabinet Office (2019) 'CRUISSE Pilot– Identifying and Addressing Uncertainties in the UK's Cyber Risk Landscape'. *NSS website.* Available at: http://cruisse.ac.uk/wp-content/uploads/2019/02/CO-Project-Final-Report-v2.pdf [Accessed: 24 July 2020].

NATO (2019) 'Remarks by NATO Secretary General Jens Stoltenberg at the

Cyber Defence Pledge Conference, London'. *North Atlantic Treaty Organisation website*. Available at: https://www.nato.int/cps/en/natohq/opinions_166039.htm [Accessed: 8th August 2020].

NATO (2020) 'Secretary General commends strong cooperation between NATO and Japan'. *North Atlantic Treaty Organisation website*. Available at: http://www.nato.int/cps/en/natohq/news_177380.htm [Accessed: 11th August 2020].

NATO Communications and Information Agency (NCIA) (2018) 'New NATO-Industry cyber partnerships signed at NITEC18'. *NATO CIA website*. Available at: https://www.ncia.nato.int/about-us/newsroom/new-natoindustry-cyber-partnerships-signed-at-nitec18.html [Accessed: 24th July 2020].

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2017) 'NotPetya and WannaCry Call for a Joint Response from International Community'. *NATO CCCDOE website*. Available at: https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/ [Accessed: 8th August 2020].

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2020) 'National Cyber Security Strategies by Country, *Strategy and Governance Documents Library.' NATO CCDCOE website*. Available at: https://ccdcoe.org/library/strategy-and-governance/ [Accessed: 24th July 2020].

Nippon Electric Company (NEC) (2017) '5 Reasons Why Japan Fell Behind in Cybersecurity'. *NEC Wisdom for Business Leaders.* Available at: https://wisdom.nec.com/en/technology/2017120601/index.html [Accessed: 26th September 2020].

Menges, F., Sperl C., and Pernul G. (2019) 'Unifying Cyber Threat Intelligence'. In: Gritzalis S., Weippl E., Katsikas S., Anderst-Kotsis G., Tjoa A., Khalil I. (eds) Trust, Privacy and Security in Digital Business. Lecture Notes in Computer Science, vol 11711. Springer.

Ministry of Foreign Affairs of Japan (MOFA) (2005) 'Agreement between the Governments of Japan and the United States of America Concerning Security Measures for the Protection of Classified Military Information'. Available at: https://www.mofa.go.jp/region/n-america/us/security/agree0708.html [Accessed: 30th September 2020].

Naughton, J. (2016) 'The evolution of the Internet: from military experiment to General Purpose Technology'. *Journal of Cyber Policy*, 1(1). pp. 5–28.

Olsen, J. (2020) 'Understanding NATO'. *The RUSI Journal*, 165(3). pp. 60–72.

Pernik, P. (2014) 'Improving Cyber Security: NATO and the EU'. International Centre for Defence Studies.

Schinagl, S. and Shahim, A. (2020) 'What do we know about information security governance? 'From the basement to the boardroom': towards digital security governance'. *Information and Computer Security*. 28(2), pp. 261–292.

Segal, A. (2018) 'When China Rules the Web'. *Foreign Affairs*, September/October. Available at: https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web [Accessed: 13th August 2020].

Shackelford, S. J. and Kastelic, A. (2015) 'Toward a State-Centric Cyber Peace?: Analyzing the Role of National Cybersecurity Strategies in Enhancing Global Cybersecurity'. *New York University Journal of Legislation and Public Policy*. 18(4), pp. 895–984. Available at: https://medium.com/freeman-spogli-institute-for-international-studies/bytes-bombs-and-spies-261564d51157 [Accessed: 25th September 2020].

Smeets, M. and H. Lin (2019). 'Chapter 4: A Strategic Assessment of the U.S. Cyber Command Vision,' in Lin, H., & Zegart, A. (Eds.). (2019). Bytes, Bombs, and Spies: The strategic dimensions of offensive cyber operations. Brookings Institution Press. Available at: https://medium.com/freeman-spogli-institute-for-international-studies/bytes-bombs-and-spies-261564d51157 [Accessed: 25th September 2020].

Stevens, T. (2012) 'A Cyberwar of Ideas? Deterrence and Norms in Cyberspace'. *Contemporary Security Policy*. 33(1), pp. 148–170.

Stevens, T. (2017) 'Cyberweapons: an emerging global governance architecture'. *Palgrave Communications*. 3(1), p. 16102.

Stevens, T. (2018) 'Cyberweapons: power and the governance of the invisible'. *International Politics*. 55(3–4), pp. 482–502.

Štitilis, D., Pakutinskas, P. and Malinauskaitė, I. (2017) 'EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis'. *Security Journal*. 30(4), pp. 1151–1168.

Stone, E. et al. (2005) *Report of Comparative Strategic Cultures Workshop (phase 1)*. Fort Belvoir: US Defense Threat Reduction Agency. Available at: https://www.files.ethz.ch/isn/129010/comparativestrategicculturesworkshop.pdf [Accessed: 8th August 2020].

Tabuchi, H. (2011) 'U.S. Expresses Concern About New Cyberattacks in Japan'. *The New York Times*. Available at: https://www.nytimes.com/2011/09/22/world/asia/us-expresses-concern-over-cyberattacks-in-japan.html [Accessed: 29th September 2020].

Tolga, İ. (2019) 'Whole-of-Government Cyber Information Sharing'. *NATO Cooperative Cyber Defence Centre of Excellence*. Available at: https://ccdcoe.org/uploads/2019/06/Cyber_Info_Sharing_Ihsan_Tolga_CCDCOE_June_2019-.pdf [Accessed: 24th July 2020].

Tsuchiya, M. (2019) 'A difficult road to international norms for cybersecurity'. *Nihon Keizai Shinbun*, 27 November. Available at: https://www.nikkei.com/article/DGXMZO52628790W9A121C1945M00/ [Accessed: 13th August 2020].

US Department of Defense, 'The Guidelines for U.S.-Japan Defense Cooperation'. April 27, 2015. https://archive.defense.gov/pubs/20150427_--_GUIDELINES_FOR_US-JAPAN_DEFENSE_COOPERATION.pdf [Accessed: 24th July 2020].

114th US Congress (2015) *Cybersecurity Information Sharing Act of 2015 ('CISA')*. Available at: https://www.congress.gov/bill/114th-congress/senate-bill/754 [Accessed: 30 Sept 2020].

von Solms, B. and von Solms, R. (2018) 'Cybersecurity and information security – what goes where?'. *Information and Computer Security*. 26(1), pp. 2–9.

von Solms, R. and van Niekerk, J. (2013) 'From information security to cyber security'. *Computers & Security*. 38, pp. 97–102.

Wagner, T., Mahbub, K., Palomar, E. and Abdallah, A. (2019) 'Cyber threat intelligence sharing: Survey and research directions'. *Computers & Security*. 87, pp.1-13.

Weiss, M. and Jankauskas, V. (2019) 'Securing cyberspace: How states design governance arrangements'. *Governance*. 32(2), pp. 259–275.

Weaver, N. (2020) 'Apple vs FBI: Pensacola Isn't San Bernardino'. *Lawfare*. Available at: https://www.lawfareblog.com/apple-vs-fbi-pensacola-isnt-san-bernardino [Accessed: 25th September 2020]

Wells II, L., Tsuchiya, M. and Repko, R. (2017) *Improving Cybersecurity Cooperation between the Governments of the United States and Japan*. Washington, DC: Sasekawa Peace Foundation USA. Available at: https://spfusa.org/wp-content/uploads/2017/02/Improved-Cyber security-cooperation.pdf [Accessed: 24th July 2020].

## 7. Appendix I. Interviewees and Research Methods Summary

| Japan Cyber Authorities or Related Entities | | |
|---|---|---|
| Prime Minister Advisor | Senior level primary advisor on IT policy | 1 |
| Japan's Minister of House of Councillors | Senior representatives from the Minister of Cyber Security | 3 |
| Japan's National Centre of Incident Readiness and Cyber security (NISC) | Senior policy and mid-level analysts | 5 |
| Japan Computer Emergency Response Team (JPCERT) | Current and former mid-level personnel | 3 |
| National Institute of Communication and Technology (NICT) | Member of the National Cyber security Research Institute | 1 |
| Japan Ministry of Defence (MOD) | Senior level cyber operations and policy military officers (05-06) | 3 |
| Ministry of Economy, Trade, and Industry (METI) | Senior level current and former members for cyber security related standards | 3 |
| Ministry of Education, Culture, Sports, Science and Technology (MEXT) | Senior level personnel on IT policy | 1 |
| Ministry of Internal Affairs and Communication (MIC) | Senior level former members for ICT policy | 1 |
| Information-Technology Promotion Agency, Japan (IPA) | Mid-level personnel | 2 |
| National Policy Agency (NPA) Office of Intelligence for<br>Cyber, Security Planning Division | Senior and mid-level technicians | 3 |
| IT-Information Sharing and Analysis Centres for Information Technology and Information Communication Technology | Senior policy and member personnel | 4 |
| Cyber Policy Academic Research | Professors in Cyber policy and ministry advisors on cyber research at Keio University | 5 |

| | | |
|---|---|---|
| UK Cyber Authorities or Related Entities | | |
| National Cyber Security Centre (NCSC) | Technical Director NCSC<br>Professors in the Academic Centre of Excellence in Cyber Security Research (ACE-CSR) sponsored by NCSC programme at Royal University and Imperial College London partnered with US and Japan (Keio) Universities for an International Cyber Strategy Curriculum | 1<br>2 |
| European Union Agency for Cyber security | Senior policy and member personnel | 2 |
| INTERPOL | Member of the cyber crime Threat Response team, Cyber Fusion Centre | 1 |
| UK Ministry of Defence | Senior officers in the Joint Forces Cyber Group Policy and Plans | 2 |
| EUROPOL | Former Executive Director | 1 |
| US Cyber Authorities or Related Entities | | |
| US Department of Defense | Advisor to DoD CIO<br>US Air Force CISO<br>US Air Force Chief DevSecOps<br>US Navy SES and military officers (05-Flag) in Cyber Policy and Planning<br>US CYBERCOM senior personnel in policy and plans | 1<br>1<br>1<br>5<br>2 |
| Cybersecurity and Infrastructure Security Agency (CISA) | International liaisons | 2 |
| HQ FBI Cyber Division and Regional Office | Senior Intel Officer and Supervisory agents | 5 |
| Former US Presidential Administration Personnel involved in Cyber Strategy Development | Former Director of National Intelligence<br>Former Principal Deputy Assistant Secretary of Defense | 1<br>1 |
| Other Cyber Relevant Entities | | |
| Private sector organisations involved Japan, US, and UK cyber operations (e.g., Toyota, Fujitsu, NEC, Hitachi, Squire Patton Boggs, Microsoft, Northrop Grumman, KPMG, PwC) | General Manager, Senior analysts, security solutions managers, legal counsel on cyber | 10 |
| Cyber security Consulting Firms (CrowdStrike, Fire Eye, McAfee, Kaspersky) | Senior threat intelligence advisors | 7 |
| Total | | 80 |