The RUSI Journal

ISSN: 0307-1847 (Print) 1744-0378 (Online) Journal homepage: https://www.tandfonline.com/loi/rusi20

Countering Cyber-Espionage and Sabotage

The Next Steps for Japanese–UK Cyber-Security Co-operation

Mihoko Matsubara

To cite this article: Mihoko Matsubara (2014) Countering Cyber-Espionage and Sabotage, The RUSI Journal, 159:1, 86-93, DOI: 10.1080/03071847.2014.895263

To link to this article: https://doi.org/10.1080/03071847.2014.895263

Published online: 17 Mar 2014.

THE RUSI JOURNAL

COUNTERING CYBER-ESPIONAGE AND SABOTAGE

THE NEXT STEPS FOR JAPANESE–UK CYBER-SECURITY CO-OPERATION

MIHOKO MATSUBARA

Cyber-security is an increasing concern for both the UK and Japan, which have recently begun to co-operate more closely in this field as part of wider efforts to revitalise bilateral ties in foreign and security affairs. Mihoko Matsubara looks at this emerging partnership and explores the benefits and drawbacks of potential future joint initiatives, suggesting how the two countries can work together to mutual benefit.

Japan and the UK are developing a closer strategic partnership rooted in both shared economic interests and national-security concerns. Surrounded by the ocean and located near a continental landmass, both countries must pursue balanced diplomacy and security strategies to meet their national defence requirements and to ensure supplies of external resources. Both are close allies of the United States and they are now looking for other security partners to counter mounting borderless threats, including cyber-attacks. It seems natural to forge such a partnership together.[1] Examining crescive Anglo-Japanese co-operation on cyber-security not only provides Japanese and UK policy-makers with a template for identifying and building previously unexplored partnerships, but also those interested in cyber-security strategy more globally, as international collaboration becomes more critical than ever in this field.

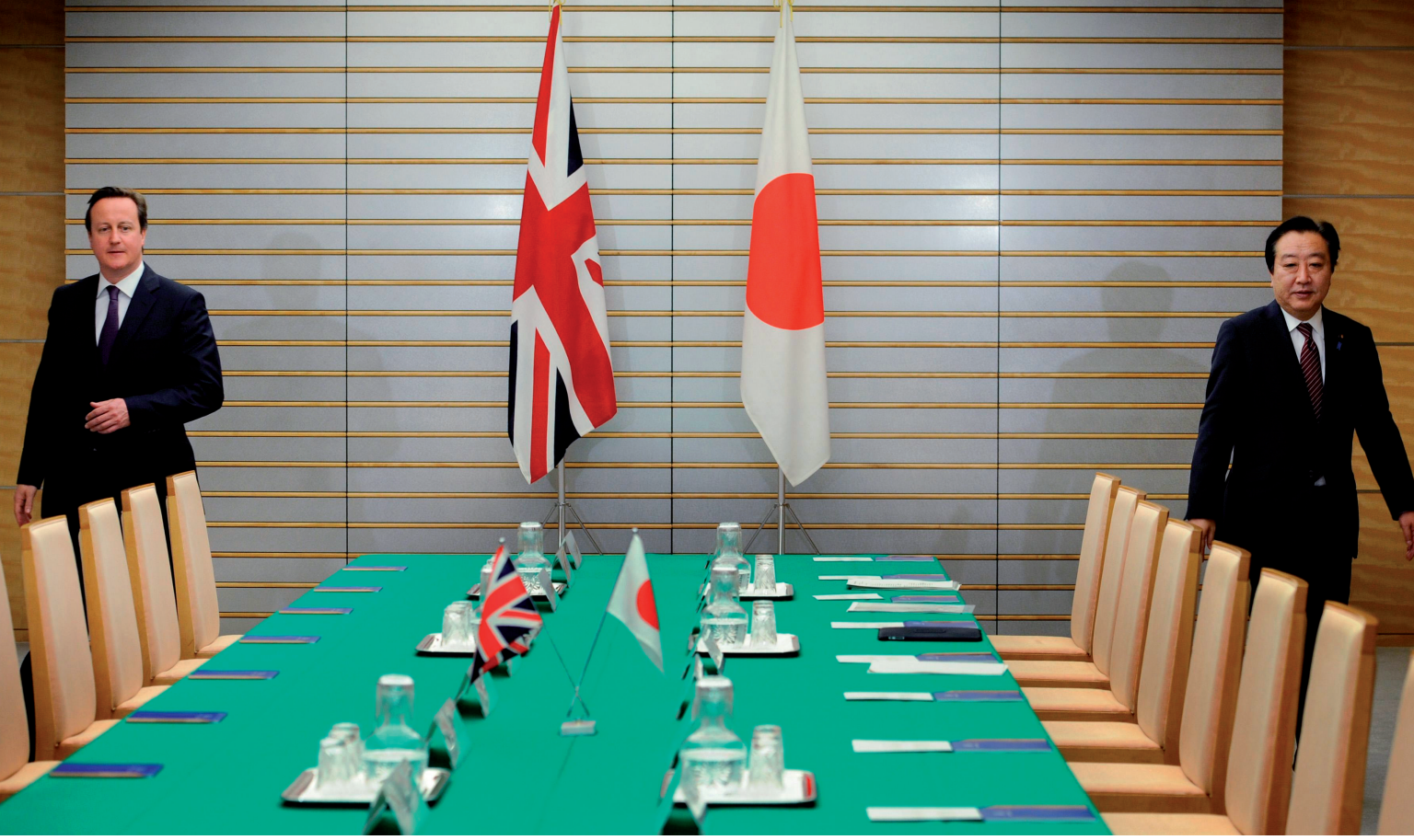
Japanese and UK economic prosperity and defence capabilities increasingly rely on information and communications technology (ICT). Japan and the UK both recognise their dependence on ICT, with each country having noted explicitly that their energy supplies, financial and medical services, as well as government and military networks, all rely on networked computer systems. Accordingly, cyber-threats now pose a high degree of risk to both countries. Since the Japanese and UK governments are pursuing stronger defence and economic partnerships, one country's vulnerability in the cybersphere could pose a risk to the other, such as disruption to business or military operations. Thus, cyber-security co-operation is crucial for their economic prosperity, social welfare and national security.

This article provides a more nuanced analysis of the burgeoning cyber-security co-operation between the UK and Japan and specific recommendations on the best steps for starting to build such a relationship. A secondary aim is to elucidate the Japanese perspective of the partnership more thoroughly to the UK public and private sectors, focusing on the challenges Japan now confronts, thereby enabling better communication between the two in the future. After examining the complexity of cyber-security and international co-operation, the following section analyses the advantages and disadvantages of the potential trajectories of Japanese–UK cyber-security co-operation. Finally, the article suggests how Japan and the UK can work together to counter the specific challenges of cyber-espionage and to ensure the protection of critical national infrastructure (CNI).

A Complex Undertaking

Cyber-security exhibits three characteristics that tend to hinder international co-operation. First, threats to cyber-security comprise a wide variety of activities such as data falsification, distributed denial of service attacks, restrictions on the free flow of information, information theft, compromised privacy, and sabotage of the functionality or operations of critical infrastructure. Information targeted through cyber-attack includes intellectual property, trade secrets and national defence-related data. Since there is no globally or even nationally agreed definition of a 'cyber-attack', governments have different perceptions of cyber-security and therefore prioritise requirements differently; thus, they struggle to set a clear threshold for the reporting of cyber-threats to one another. Currently, there is an agreement between many governments to report any cyber-attack, but such vagueness could result in the sharing

 DOI: 10.1080/03071847.2014.895263



The April 2012 meeting between the prime ministers of Japan and the UK initiated negotiations on a government-to-government information security agreement. *Courtesy of Stefan Rousseau/AP Photo.*

of a massive amount of relatively trivial information, including about minor attacks or unfiltered indicators provided by security tools. Even minor losses of confidence in the utility of information-sharing could then easily make some officials hesitant to pass on further information.

Second, cyber-security issues affect nearly every aspect of governance and economic activity. Even though cyber-threats are not necessarily visible, they have already had a diverse impact on all major sectors of commerce, finance, industry, technology and national defence. This wide scope of potential targets forces states to empower multiple agencies or ministries with responsibilities for cyber-security and the protection of national interests. At the same time, that multifaceted governmental structure makes it difficult to take an overarching, unified approach to dealing with cyber-threats. As such, it becomes difficult for any government to co-ordinate policy among different stakeholders in both public and private sectors and to prioritise assets for protection – a problem exacerbated by the limited resources available due to the current economic malaise and budgetary austerity. With such complications hindering progress within individual countries, it is naturally even harder to co-ordinate between them.

Third, the borderless and cross-sectoral nature of cyber-attacks makes international co-operation crucial. In fact, every strategically and economically conscious government now understands the necessity of co-operation to counter organised cyber-crime and state-sponsored cyber-attacks. They are also well aware that information-sharing is important in mitigating the full range of cyber-threats.[2] Yet this does not necessarily mean that governments have become effective in using the information available to weed out vulnerabilities or to minimise contagion from potential or ongoing damage. Also, more risk-averse officials often fear (sometimes rightly so) that intergovernmental information-sharing could disclose sensitive intelligence about network vulnerabilities, intellectual property or national defence. Thus, it is indispensable to build confidence in information assurance and cyber-defence capabilities between organisations and individuals sharing capabilities, data and insights via both formal and informal channels. These two layers of communication and co-ordination function symbiotically, allowing participants to better understand issues and devise solutions outside the official scope of formalised partnership structures when those fail or prove inadequate in the face of unanticipated developments or exigencies.[3]

To overcome these complexities, therefore, any sound scheme for international cyber-security co-operation must begin with at least the following two foundational steps: detailed scoping of the area for co-operation, including at least the general objectives, specific types of information to be shared, according to which criteria and under what circumstances; and the completion of a mutually credible agreement on information assurance to protect national secrets. The first of these steps has proven continuously difficult but remains unavoidable. Since cyber-threats have become a popular topic of significant consequence, it is relatively easy for officials to choose the generic issue of 'cyber-security' as a desirable focus point for a strategic partnership. It is harder to operationalise these efforts. Given that different countries have different interests – such as privacy, regulations, and the prioritisation of security issues – it is often difficult to co-ordinate them

to reach a consensus. Operationalisation includes, at minimum, the establishment of a structured way of sharing information periodically, a mutual commitment to ad hoc information-sharing in emergencies, and instantiation through joint cyber-exercises and simulations. For these efforts, it is crucial to establish robust information assurance to manage risks associated with sharing, storing and using sensitive information.

Risks and Opportunities

To take the first step, it is helpful if those countries seeking a partnership share political values or at least strategic interests. Japan and the UK share many of their core political values such as democracy, human rights and a commitment to the rule of law. This makes it easier for the two governments to collaborate on legal issues associated with cyber-security. In addition, both Japan and the UK advocate wider international co-operation on cyber-security, given that cyber-attacks pose grave threats to global security. Japan's first cyber-security strategy, the Information Security Strategy for Protecting the Nation, published in 2010, acknowledges borderless cyber-threats and the necessity to expand international co-operation to co-ordinate between the different policies, laws, regulations and norms of each country.[4] The UK's 2010 National Security Strategy, meanwhile, refers to cyber-attacks as a Tier One risk,[5] and the UK Cyber Security Strategy of November 2011 also declares an intention to promote international co-operation.[6]

Furthermore, although they are not formal security allies in the sense of being bound by a bilateral security treaty or mutual membership in a multinational alliance, the Japanese and UK governments have been developing tighter security relations in recent years through reconstruction efforts in Afghanistan and anti-piracy operations in the Gulf of Aden. The trust fostered through those operations resulted in a joint statement being issued in April 2012 by the two countries' respective prime ministers, Yoshihiko Noda and David Cameron, to 'reconfirm the distinctive importance of the leading strategic partnership' between the two countries.[7] UK Foreign Secretary William Hague also repeatedly emphasises the solidity of the bilateral relationship, describing Japan as 'one of [UK's] closest partners in Asia'.[8]

Japan and the UK share many core political values

The meeting between the two prime ministers in April 2012 also marked the beginning of a sixteen-month process of negotiations on a government-to-government information security agreement.[9] In June 2012, the Japanese Ministry of Defense (JMoD) and the UK Ministry of Defence (MoD) signed a joint memorandum on defence co-operation, as recommended in the prime ministerial joint statement. The document indicates that the ministries will uphold rigorous standards to protect information exchanged between them and that neither country will pass the information on to a third country without the other ministry's consent.[10] This was followed – more than a year later, in July 2013 – by a formal agreement between the two countries that goes one step further by outlining the protection of secrets shared at the governmental level, rather than merely at the ministerial level.[11]

From the UK's perspective, the single greatest concern over information assurance would likely pertain to the lack of an anti-espionage law in Japan. Indeed, some US security experts have already expressed worries about this.[12] The Japanese government tried to enact such a law in 1985 but failed due to strong opposition by the Japan Federation of Bar Associations, liberal political parties and the media, which were worried about any potential limitation on freedom of the press because of the dark pre-war legacy of censorship in Japan. The Japanese government has openly recognised the necessity of more robust information assurance and in December 2010 duly established a committee to implement this goal, headed by the chief cabinet secretary. The third meeting of the committee submitted a report to the government in August 2011 that pointed out that information leaks due to foreign espionage activities have already occurred. Tellingly, the report also argued that legislation to protect secrets is crucial to deter information leaks and to enhance information-sharing with other governments.[13]

More recently, there has arisen a promising movement in Japan for improving information assurance by imposing more severe punishments for non-compliance or violation. In December 2013, the Diet passed a bill to protect classified information regarding counter-intelligence, counter-terrorism, diplomacy and national defence by strengthening penalties for government officials who leak secrets related to defence, diplomacy or public safety, increasing the one-year prison sentence specified under the current National Public Service Law to up to ten years.[14] The current maximum penalty under the Self-Defense Forces (SDF) Law is up to five years in prison, and it is up to ten years if the defence secrets leaked are subject to the Act to Protect Classified Information under the Japan–US Mutual Defense Assistance Agreement. Although the law does not take effect until December 2014, the determination of the Shinzo Abe administration should be sufficiently reassuring to the UK government for it to begin scoping the level of classified information to share with its Japanese counterpart.

Bilateral Cyber-Security Co-operation

It has been over a year since Tokyo and London officially initiated their cyber-security co-operation agreement. The April 2012 joint statement proclaimed the intention to 'strengthen bilateral consultation on issues related to cyberspace and cooperate internationally' on the establishment of a cyber code of conduct. Another important element of co-operation is the development and production of defence equipment,[15] formalised in the joint memorandum on defence co-operation in June 2012 and agreed to 'foster a long-term mutually beneficial partnership' on various emerging fields including cyber-security.[16]

In late June 2012, the two governments held their first cyber-security dialogue in Tokyo. Although the details of the conference's content remain undisclosed, both sides seem to have taken a whole-of-government approach, extending the agenda and the invitations beyond the sphere of national defence. Among the delegates were officials from the Japanese Ministry of Foreign Affairs, the UK Foreign Office and the Cabinet Offices of both countries. During the dialogue, the two governments introduced their unilateral efforts to counter cyber-crime. The participants also discussed the challenges of confronting cyber-threats as national security problems as well as how to establish an international code of conduct for cyberspace in order to explore specific areas on which to co-operate.[17] Although Japanese Foreign Minister Fumio Kishida and UK Foreign Secretary William Hague agreed in October 2013 to resume working-level dialogue regarding cyber-security as soon as possible,[18] the second such meeting has not yet been announced and, at the time of writing, it remains unknown when it will be held.

Next Steps

Both governments are increasingly alarmed by cyber-espionage targeting the public and private sectors as well as potential cyber-sabotage of critical infrastructure. Cyber-espionage and sabotage are the two most important areas on which Japan and the UK could benefit strongly by working together. Both governments refer to these two broad issues in their respective national cyber-security strategies. The UK's 2011 Cyber Security Strategy recognises the significance of these threats and argues the necessity of establishing public–private partnerships in order to share information and decrease vulnerabilities in critical infrastructure.[19] Japan's 2013 Cyber Security Strategy also stresses mounting risks of information theft and disruption to the operation of critical infrastructure. The strategy document argues that cyber-attacks can exploit the vulnerability of critical infrastructure control systems and paralyse their operations, with the resultant blackout or disruption to communication systems potentially causing widespread turmoil.[20]

Countering Cyber-Espionage

Both the Japanese and the UK's defence industrial bases have been frequent targets of cyber-espionage. A Japanese newspaper reported in September 2011 that unknown assailants had breached the networks of Mitsubishi Heavy Industries, one of Japan's largest defence contractors, and infected eighty computers, probably to steal information on missiles, nuclear power plants and submarines.[21] Following that, the media discovered that other major defence contractors, such as IHI and Kawasaki Heavy Industries, had also been targeted. It was reported in March 2012 that computers at the British firm BAE Systems had been compromised, for at least eighteen months, by Chinese hackers with the aim of stealing information regarding the design, electronics systems and performance specifications of the F-35.[22] These reports were pertinent to Japanese security because in December 2011, the Japan Air Self-Defense Force (SDF) had decided to procure the F-35 as its next-generation fighter aircraft. Similar incidents in the future would ruin the capability of the SDF and UK armed forces to take full advantage of military equipment that is jointly developed by the two countries and could hinder the performance of their unilateral or joint operations.

Although non-defence-related companies, ministries and universities are also targeted,[23] the most pressing concern should be to protect defence-related organisations from cyber-attack. Also, the two governments can help Japanese businesses in the UK and vice versa by alerting them to cyber-threats. For information-sharing on defence, the Japanese and British MoDs should serve as one another's trusted point of contact based on the bilateral agreement to protect secrets for two reasons. First, one point of contact in each country would avoid overlapping exchanges of the same information as well as facilitating information delivery. Second, the ministries would be able to ensure secure communications to protect sensitive information better than industry would. Finally, each ministry needs to co-ordinate a format, language and type of information to share with the other in order to ensure the anonymity of targeted companies if necessary.

Both countries initiated a public–private partnership to share information on cyber-threats in July 2013. The UK Defence Cyber Protection Partnership (DCPP) released its list of stakeholders, which includes the UK's signals-intelligence body GCHQ and the MoD on the government side, and the Centre for the Protection of National Infrastructure (CPNI) and BAE Systems on the private-sector side. It is worth noting that GCHQ is a key player in UK cyber-security and the wider UK intelligence community is more visible in its support for private-sector cyber-security interests than its Japanese counterpart.

Cyber-espionage and sabotage are the two most important areas of collaboration

This secrecy reflects much greater constraints on the JMoD, the SDF and the new cyber-security public–private partnership, the country's Cyber Defense Council (CDC) under the constitution. Since Article 9 of the Japanese constitution prohibits Japan from possessing offensive military capabilities, some politicians – from the Social Democratic Party, for example – have argued that the SDF is illegal. Concordantly, the JMoD and SDF have been hesitant to take a proactive role in national and international security and, as a result, the armed forces' abilities in the realms of national defence and intelligence have been constrained. Another consequence is that the JMoD and SDF are only allowed to protect their own internal networks because it would be too controversial were they to defend outside networks.

Another explanation for this secrecy was made clear when the CDC announced that it would not reveal the identity of its members – its explanation being that it wanted both to ensure frank discussions and open information-sharing, and

to avoid any negative impact on the companies' business operations.[24] Such secrecy, though well-intentioned, could prohibit the JMoD from sharing specific information regarding cyber-attacks against Japanese defence firms with the UK. Furthermore, the asymmetry between the responsibilities and visibility of the Japanese intelligence community and its British counterpart – in terms of cyber-security – could hinder bilateral co-operation and information-sharing in support of both the public and private sectors. To operationalise co-operation, the reform of Japan's intelligence capabilities is essential.[25]

In addition to defence-related information, the two countries would benefit from exchanging information on cyber-attacks that could harm the property of Japanese or UK citizens (or companies) residing in the other country. The stealth and sophistication of cyber-espionage makes it harder for victims or potential victims to notice a threat – or, indeed, an actual attack – and it is useful for the two countries to share their observations of the trends in targets and tactics to minimise future damage. Around 2012, for example, attackers started modifying their infection tactics from spear-phishing – e-mails with malware attachments – to so-called 'watering hole attacks', which infect websites that are likely to be visited by private individuals or members of industry or organisations of interest to the attackers, leading eventually to compromises of the target's computer.[26] Even though some Japanese organisations post information about hacking activity on their websites, it is usually only available in Japanese. English-speaking audiences who work in Japan or work closely with the Japanese would therefore find it helpful if Japan's National Information Security Center (NISC) were to provide English alert newsletters.[27]

Furthermore, the UK can help Japan by sharing the lessons it has learned from dealing with cyber-threats during the 2012 Olympic and Paralympic Games – which are all the more pertinent as Tokyo prepares to host its own Olympic Games in 2020. For example, prior to the opening ceremony of the London Olympic Games, the organiser received a credible warning about potential cyber-attacks on essential electricity infrastructure, although such an incident was fortunately averted.[28] Along with potential disruption to critical infrastructure, hosting the Olympic Games could prompt attackers to create scam websites to sell fake tickets to steal information. For instance, in July 2012, during the run-up to the London Games, a major security firm, McAfee, warned about phishing emails luring victims into a scam by informing them that they had won a game-related lottery – and £950,000.[29]

The UK can share lessons from the 2012 Olympic Games

Due to the various types of possible cyber-threats associated with the Olympic Games, from online fraud to sabotage, it would require multiple levels of classification to share information between Japan and the UK, while several governmental organisations and the Tokyo Metropolitan government would need to be involved in order to deal with ICT, infrastructure, intelligence and law enforcement. Although Japan currently lacks a security-clearance system that encompasses the entire central government, the new state-secrets law would provide a security-clearance system and also a relevant background-check system to cover central government officials, government contractors and local police officers.[30] Thus, it is necessary for the central government to decide on whether it will provide security clearance to the top leadership of the Tokyo metropolitan authorities in order to share classified information regarding the Olympic Games, and whether it will offer declassified or unclassified information to metropolitan non-law enforcement officials. The central government also needs to consult with its UK counterpart about how to share lessons learned from the London event and advice with metropolitan authority officials – whether or not classified information is to be included or limited to only declassified or unclassified material. This is crucial to fostering the same situational awareness of potential contingency or risks across both levels of government.

Countering Cyber-Sabotage

There are two compelling reasons for UK–Japanese co-operation on cyber-security. First, even though there have been no reports of intentional disruption to either Japanese or UK critical infrastructure via cyberspace, such incidents have occurred elsewhere, some of which resulted in physical harm to individuals or in disruption to business operations. For example, in Poland in 2008, having modified a TV remote control in order to hack the control system of the local tram network in Lodz, a teenage boy changed some of the track points – with the result that four trams were derailed and at least twelve people were injured.[31]

Second, the UK may increasingly import infrastructure from Japan, in line with Prime Minister Shinzo Abe's goal of tripling the value of infrastructure exports to 30 trillion yen by 2020 as part of his strategy to stimulate the economy.[32] As of January 2014, there are two contracts between the two countries. Hitachi, a giant of Japanese industry, acquired Horizon Nuclear Power from RWE and E.ON in October 2012 and plans to construct up to six nuclear reactors at Wylfa on Anglesey and Oldbury in Gloucestershire.[33] Meanwhile, in July 2013, Hitachi Rail Europe won a contract worth £1.2 billion from the UK Department of Transport to build 270 train carriages in the UK, for use on its East Coast Main Line.[34] It is crucial for the two countries to ensure both cyber and physical security of infrastructural projects.

Co-operation in this field should go relatively smoothly because Japan and the UK have overlapping definitions of critical infrastructure. Both countries include communications, medical services (emergency services and health in the UK), financial services, government, transportation and water in their definitions of critical infrastructure. They differ in their classification of energy and food, but these are minor differences.

Japan has recently begun to take extra steps to ensure the cyber-security

of the control systems of its critical infrastructure. Although European countries and the US require a certificate for system assurance when they import infrastructure, Japan does not currently have a domestic body for verifying, and issuing certificates for, system assurance in relation to infrastructure exports.[35] Thus, Japanese companies have to rely on foreign institutes – and the process takes time and entails significant costs. However, in May 2013, the Japanese government established the Control System Security Center (CSSC) in Miyagi Prefecture, in northern Japan, to develop technologies that will secure control systems for critical infrastructure and to establish a cyber-security certificate. To help it achieve this, the centre has seven plants including a car manufacturing plant, chemical plant and thermal power plant to conduct exercises or simulations to deal with cyber-attacks.[36]

The largest challenge the centre faces is the scarcity of cyber-security experts with knowledge of the latest trends in adversaries and malware usage, and who can create realistic simulation scenarios. Furthermore, since a large number of critical infrastructure companies use remote control for reasons of efficiency, a simulation that models this is also a must. Operators of ICT systems, for example, need to be prepared to deal with cyber-attacks on remote-controlled critical infrastructure with nobody on site.[37] Given that the CSSC just commenced operations, it will necessarily take time to develop pertinent capabilities and sufficient manpower before it can issue certificates. However, it is still a welcome first step for Japan to invest so extensively with the aim of bolstering the cyber-security posture of critical infrastructure systems overall and of infrastructure for export in particular.

For bilateral co-operation in this regard, the main points of contact would be the NISC in Japan and the Office of Cyber Security and Information Assurance (OCSIA) in the UK, although other ministries and private companies are involved in the protection of critical infrastructure. Indeed, the NISC and OSCIA should serve as co-ordinators between the two countries to explain current and future policy and regulations related to critical infrastructure to one another. However, to help the CSSC to accelerate its efforts in establishing Japan's own certificate, the CPNI should also notify the NISC of cyber-security requirements for UK critical infrastructure as well as lessons learned from previous cyber-attacks (attempted or successful). Such information would be especially useful if it pertains to the UK's railway network and nuclear plants, given these are the subjects of the current two contracts. Although regular information-sharing on cyber-threats requires confidence-building between the organisations and people involved – which can take time – the two contracts already signed would enable them at least to begin more concrete and durable efforts that could lead to a long-term, successful partnership.

Conclusion

In the time since the official agreement to pursue cyber-security co-operation was signed, Japan and the UK have made some progress at the strategic level, such as the conclusion of the bilateral agreement to protect classified information and the convening of the first cyber-security dialogue. The Abe administration's efforts to enforce the law to protect national secrets are also encouraging in terms of improved information assurance in Japan – and it potentially leads to the sharing of sensitive information between Japan and the UK. Yet there is still a long way to go to operationalise this co-operation at the tactical level, partly because confidence-building takes time and also because both countries are struggling to establish better domestic cyber-security. Especially from the Japanese perspective, limited intelligence capability and visibility could hinder bilateral co-operation and thus reform in this area is crucial.

Both countries face grave risks from cyber-espionage campaigns and both recognise the potential threats to their critical infrastructure. Momentum in the promotion of bilateral collaboration is fuelled by several promising factors such as opportunities for the joint development and production of military equipment, the Tokyo Olympic Games in 2020, and Japan's infrastructure exports to the UK – with two contracts already in place and potentially more to come. Since 2013 witnessed rapid reforms in both countries in relation to cyber-security, the Japanese and UK governments are now well-placed to incorporate these unilateral efforts, developing a more robust bilateral cyber-security co-operation. ■

Mihoko Matsubara is a cyber-security analyst and Adjunct Fellow, Pacific Forum CSIS, Honolulu.

Notes

1 Julian Ryall, 'Japan and Britain Cement Defense Ties', *Deutsche Welle*, 18 October 2013.

2 White House, 'The Comprehensive National Cybersecurity Initiative', January 2008, <http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>, accessed 25 January 2014.

3 Author interview with Eli Jellenc, Senior Manager, Cyber Intelligence, iDefense Information Security, Verisign, 29 August 2013.

4 Information Security Policy Council, '*Kokumin wo mamoru joho sekyuriti senryaku* [Information Security Strategy for Protecting the Nation]', 11 May 2010, pp. 2, 5, <http://www.nisc.go.jp/active/kihon/pdf/senryaku.pdf>, accessed 22 January 2014.

5 The National Security Council regards Tier One risks as the 'highest priority for UK national security looking ahead, taking account of both likelihood and impact'; see HM Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Cm 7953

(London: The Stationery Office, October 2010), p. 27.

6 UK Cabinet Office, 'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World', November 2011, p. 36, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>, accessed 22 January 2014.

7 Japanese Ministry of Foreign Affairs (MOFA), 'Joint Statement by the Prime Ministers of the UK and Japan: A Leading Strategic Partnership for Global Prosperity and Security', press release, 10 April 2012, <http://www.mofa.go.jp/region/europe/uk/joint1204.html>, accessed 22 January 2014.

8 Foreign and Commonwealth Office, 'Announcement: Foreign Secretary Meets Japanese Foreign Minister', press release, 3 May 2011; Foreign and Commonwealth Office, 'News Story: Foreign Secretary Welcomes Japanese Foreign Minister to London', press release, 11 April 2013.

9 MOFA, 'Joint Statement by the Prime Ministers of the UK and Japan'.

10 Japanese Ministry of Defense (JMoD), 'Memorandum between the United Kingdom Ministry of Defence and the Japan Ministry of Defense Relating to Defence Cooperation', 3 June 2012, <http://www.mod.go.jp/j/press/youjin/2012/06/03_memo.pdf>, accessed 22 January 2014, pp. 3–4.

11 MOFA, 'Agreement between the Government of Japan and the Government of the United Kingdom of Great Britain and Northern Ireland on the Security of Information', 4 July 2013, <http://www.mofa.go.jp/mofaj/files/000016358.pdf>, accessed 25 January 2014.

12 Author interviews with US security experts in Washington, DC, December 2012.

13 Prime Minister of Japan and His Cabinet, 'Shiryo 3: himitsu hozen no tame no hosei no arikata nit suite (hokokusho) no gaiyo [Handout 3: How to Establish Legislation to Protect Secrets (Report)]', 8 August 2011, <http://www.kantei.go.jp/jp/singi/jouhouhozen/dai3/siryou3.pdf>, accessed 28 July 2013, p. 1.

14 *Asahi Shimbun*, 'EDITORIAL: Secrets Protection Bill Should Not Infringe on the People's Rights', 26 August 2013, <http://ajw.asahi.com/article/views/editorial/AJ201308260026>, accessed 22 January 2014; Prime Minister of Japan and His Cabinet, 'Main Points of the Act on the Protection of Specially Designated Secrets', 13 December 2013, <http://www.kantei.go.jp/jp/topics/2013/headline/houritu_gaiyou_e.pdf>, accessed 25 January 2013.

15 MOFA, 'Joint Statement by the Prime Ministers of the UK and Japan'.

16 JMoD, 'Memorandum between the United Kingdom Ministry of Defence and the Japan Ministry of Defense Relating to Defence Cooperation', p. 3.

17 MOFA, '*Nichiei saiba kyogi no kaisai ni tsuite* [Japan–UK Cyber Dialogue Was Held]', 20 June 2012, <http://www.mofa.go.jp/mofaj/area/uk/juk_cyber1.html>, accessed 22 January 2014.

18 *Sankei Shimbun*, '*Nichiei Gaisho, saiba nado boei kyoryoku suishin de icchi 2 dome no senryaku taiwa* [Japanese Foreign Ministers and British Foreign Secretary Agreed to Expand their Defence Co-operation on Cyber during their Second Strategic Dialogue]', 16 October 2013, <http://www.sankei.jp.msn.com/politics/news/131016/plc13101617190021-n1.htm>, accessed 25 January 2014.

19 UK Cabinet Office, 'The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World', November 2011, <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>, accessed 22 January 2014, pp. 5, 15, 23, 32.

20 Information Security Policy Council, '*Saiba sekyuriti senryaku – sekai wo sossen suru kyojin de katsuryoku aru saiba kukan wo mezashite* – [Cyber Security Strategy – Aiming to Become a Global Leader and Achieve a Robust and Vibrant Cyberspace]', 10 June 2013, <http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf>, accessed 22 January 2014, pp. 5, 7.

21 *Reuters*, 'Japan's Defense Industry Hit by its First Cyber Attack', 19 September 2011.

22 *Australian*, 'Security Experts Admit China Stole Secret Fighter Jet Plans', 12 March 2012, <http://www.theaustralian.com.au/news/world/security-experts-admit-china-stole-secret-fighter-jet-plans/story-fnb64oi6-1226296400154>, accessed 22 January 2014.

23 John E Dunn, 'Japanese Finance Ministry Uncovers Major Trojan Attack', *Computerworld*, 24 July 2012, <http://www.computerworld.com/s/article/9229534/Japanese_Finance_Ministry_uncovers_major_Trojan_attack>, accessed 22 January 2014; Helen Warrell, 'MI5 Warns Universities on Cyber Spying', *FT.com*, 10 April 2013.

24 Michael Crosby, 'MOD Announce Partnership with UK Firms to Tackle Cyber Threats', 5 July 2013, <http://www.dcicontracts.com/DCIblog/2013/07/05/mod-announce-partnership-with-uk-firms-to-tackle-cyber-threats/>, accessed 22 January 2014; JMoD, '*Cyber Defense Renkei kyogikai (CDC) no secchi torikumi nit suite* [The Establishment and Purpose of the Cyber Defense Council (CDC)]', July 2013, <http://www.mod.go.jp/j/approach/others/security/cyber_defense_council.pdf>, accessed 22 January 2014, pp. 3–4.

25 Author interview with Eli Jellenc.

26 Will Gragido, 'Lions at the Watering Hole – The "VOHO" Affair', RSA blog, 20 July 2012, <https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/>, accessed 22 January 2014.

27 The NISC is placed under the Cabinet Secretariat to serve as a focal point to craft cyber-security policy and co-ordinate information-sharing with domestic and international partners.

28 Gordon Corera, 'The "Cyber-Attack" Threat to London's Olympic Ceremony', *BBC News*, 8 July 2013.

29 Francois Paget, 'Scams Surround London Olympics', McAfee Labs, 13 July 2012, <https://blogs.mcafee.com/mcafee-labs/scams-surround-london-olympics>, accessed 22 January 2014.

30 Japanese Cabinet Intelligence and Research Office, 'Shiryo 1: Waga kuni no joho kino [Material 1: Our Country's Intelligence Capabilities]', 24 February 2009, <http://www.kantei.go.jp/jp/singi/ampobouei2/dai4/siryou1.pdf>, accessed 10 July 2013, p. 5; Prime Minister of Japan and His Cabinet, '*Tokutei himitsu no hogo nikansuru horitsu* [State-Secrets Law]', 13 December 2013, <http://www.kantei.go.jp/jp/topics/2013/headline/houritu_joubun.pdf>, accessed 25 January 2014.

31 John Leyden, 'Polish Teen Derails Tram after Hacking Train Network', *Register*, 11 January 2008, <http://www.theregister.co.uk/2008/01/11/tram_hack/>, accessed 22 January 2014.

32 Keiko Ujikane and Toru Fujioka, 'Japan Output Gains as Tokyo Prices End Four-Year Slide: Economy', *Bloomberg*, 31 May 2013.

33 Geraint Jones, 'Anglesey in Line for Wylfa Cash Boost', *News North Wales*, 17 July 2013, <http://www.newsnorthwales.co.uk/news/124736/anglesey-in-line-for-wylfa-cash-boost.aspx>, accessed 22 January 2014.

34 *Reuters*, 'UPDATE 1-Japan's Hitachi Wins $1.8 bln UK Train Carriage Order', 18 July 2013.

35 Mitsubishi Research Institute, '*Hokoku shiryo Shiryo 1-6: Inhura yushutsu ni oite shiteki sareru kadai to jirei* [Research Report 1-6: Challenges to Export Infrastructure and Relevant Examples]', 31 January 2011, <http://www.soumu.go.jp/main_content/000101429.pdf>, accessed 22 January 2014, pp. 10–12.

36 *Nihon Keizai Shimbun*, '*Seigi no hakka' yosei saiba mogi kobo, Miyagi ni shisetsu* [A New Facility to Train White Hat Hackers who Can Counter Cyber-Attacks]', 2 June 2013, <http://www.nikkei.com/article/DGXNASDD280HT_Y3A520C1XX1000/>, accessed 22 January 2014.

37 Hitachi Systems, 'Control System Security Center was Established in Northern Part of Japan', 4 June 2013, <http://www.shield.ne.jp/ssrc/topics/SSRC-ER-13-023-en.html>, accessed 22 January 2014.