2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges & State Practices Across Asia and Europe

Sergei Boeke LL.M.
Leiden University Centre for Terrorism and Counterterrorism
The Hague, The Netherlands

Matthijs A. Veenendaal
NATO Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia

Caitríona H. Heinl
Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Singapore

Abstract: While many states are developing national cyber security strategies, the exact role and responsibilities of the armed forces in cyberspace often remain unclear. Although attention has been devoted to acquiring specific technical capacities and expertise to act in cyberspace, decision-making processes, doctrines for deployment, and procedures generally lack systematic analysis. The first part of this article therefore focuses on whether militaries in their own national context contribute to defensive cyber security tasks. Common national challenges are identified, as are approaches that potentially improve cyber security through better civil-military cooperation. The article then examines the organisational structures in place across Asia and Europe to enable better international military cooperation for cyber related incidents. It outlines how international cooperation might assist a better exchange of information to increase cyber defence effectiveness, specifically between Asia and Europe.

Keywords: *cyber defence, civil-military relations, international military cooperation, Europe, Asia*

1. INTRODUCTION

As cyber security is increasingly conflated with national security, there is debate on whether cyberspace is being militarised.[1] Armed forces across the globe are investing in their capacity to defend their networks and systems, and increasingly, preparing to conduct military operations in cyberspace. While alarmists in academia and politics warn of the threat of 'a digital Pearl Harbor' or a 'cybergeddon', potentially paralysing a connected society,[2] the question of how armed forces can or should contribute to enhancing and protecting national and international cyber security, outside of an armed conflict, has not been fully answered yet and has thus far received limited academic attention.

This article therefore aims to investigate the challenges faced by different European and Asian nations in defining the role of the armed forces regarding cyber security and how these are formulated in official national documents. The focus lies exclusively on the militaries' defensive tasks, excluding possible 'offensive operations'. This article builds on the results of a workshop organized by the S. Rajaratnam School of International Studies (RSIS), Singapore and Leiden University Centre for Terrorism and Counterterrorism (CTC), which was held in Singapore in November 2014 and made possible by the ministry of defence of the Netherlands.

The article is divided into two sections. The first section examines the military's role in national cyber security while the second section considers the structures in place across Asia and Europe to enable better international military cooperation for cyber related incidents between the two regions.

2. THE MILITARY'S ROLE IN NATIONAL CYBER SECURITY

This section focuses on the challenges involved in defining and clarifying the responsibilities of the armed forces regarding the protection of national security and how these relate to civilian authorities. Common national challenges are identified, as are approaches that potentially improve cyber security through better civil-military cooperation.

The growing dependence of critical infrastructure on digital technology has been generally recognized and, consequently, the protection of national critical infrastructure is a central tenet in most cyber security strategies and policies. The way in which cyberspace is structured and governed means that the digital domain presents several challenges when it comes to protecting national security. In cyberspace, the classical distinctions between military and civil, public and private and national and international actors are less clear-cut. For instance, as critical infrastructure is predominantly run by the private sector in most countries across Europe and Asia, although not all, some form of public-private partnership for crisis management and

1 See for instance Ronald J. Deibert, '*Black Code: censorship, Surveillance and the increasing Militarization of Cyber space*', Journal of International Studies, December 2003 vol. 32 no. 3 501-530 and Myriam Dunn Cavelty (2012), '*The Militarisation of cyberspace, Why less may be better*', Proceedings of the 4th International Conference on Cyber Conflict (Tallinn, 2012).

2 See for instance Richard Clarke and Robert Knake, '*Cyber War: The Next Threat to National Security and What to Do About It*', (New York, 2010) and Leon Panetta, *Defending the Nation from Cyber Attack*", speech delivered at Business Executives for National Security, New York, October 11, 2012. http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1728 [accessed March 2015].

incident response is necessary.[3] While many approaches are possible, ranging from stimulating self-regulation to interventionist government policies, complex issues remain related to the way in which governments address their responsibility for the protection of critical infrastructure.[4]

In both Asia and Europe, different ministries are responsible for coordinating cyber security issues and critical infrastructure protection. These ministries range from the ministry of justice (as is the case in the Netherlands and Indonesia), the ministry of the interior (Estonia and Germany), the ministry of technology or information technology (India, Malaysia and Thailand), to the ministry of defence (Denmark). The varied way of conferring responsibility has its origins in different factors, such as historical context, domestic considerations, and wider geostrategic concerns. The consequences, however, are significant as the legal mandate can vary per sector, with ministries of the interior or home affairs predominantly concerned with public order, ministries of justice with law enforcement and ministries of defence with national security. From this perspective it would be logical for a country which considers cyber crime the most serious threat to mandate the justice ministry with the coordination of cyber security, while one fearful of state sponsored espionage or cyber conflicts should be more inclined to give a lead role to defence organisations. While more research is certainly warranted in this area, it appears that, although national policies and strategies certainly reflect perceived cyber threats, the institutional embedding of roles and responsibilities in the cyber domain often follows a different logic and is more a result of specific political and organizational traditions and processes.

National perspectives on whether to focus on the opportunities or threats of cyberspace also differ within both Asia and Europe. In Asia, for instance, countries such as Laos and Cambodia have a low ratio of Internet connectivity, and, given their less cyber dependent critical infrastructure, their cyber security policies are developed more from the perspective of the opportunities these offer for economic growth. India also has a cyber policy that focuses strongly on the economic policies.[5] Some countries like Spain and Thailand seem most concerned about cyber crime and malicious cyber activities from non-state actors. Although cyber crime is described by many countries as the major threat in Asia and Europe, simmering interstate tensions and a host of cyber incidents that have been kept from public view imply that the securitisation[6] of cyberspace is perhaps more acute but less acknowledged in Asia. South Korea, for example, is formally still at war with North Korea, and, together with Japan, the country has been the target of cyber attacks, indicating North Korean involvement.[7] Central to the Asian geopolitical context is the position of China and the perceived United States pivot to the Asian Pacific, and several countries in Southeast Asia are involved in long-standing territorial or maritime disputes with China. Some countries estimate that the most serious threat emanates from state-sponsored cyber activities. Irrespective of official threat analyses, the distinction between cyber

3 Myriam Dunn-Cavelty & Manuel Suter, 'Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection', *International Journal of Critical Infrastructure Protection*, Volume 2, Issue 4, December 2009, pages 179–187.

4 Ibid.

5 National Cyber Security Policy of India (2013). Retrieved in March 2015 from: http://deity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20(1).pdf.

6 Securitization means that "[an issue] is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure." Security "frames the issue either as a special kind of politics or as above politics." (in *Security: A New Framework for Analysis*, Barry Buzan et al. 1998, p. 23).

7 See for instance the Choe Sang-Hun, '*Computer networks in South Korea are paralyzed by cyber attacks*', The New York Times, 20 March 2013.

crime and state-sponsored activities is often blurred in practice, with attribution being costly in terms of time and effort.[8]

Since there is no consensus on the threat landscape and there is a large diversity of political systems and cultures, there is no single institutional construction that can be identified as a role model for others. Various issues are, however, addressed in similar ways. What stands out, for instance, is that when nations define the roles and responsibilities of the armed forces vis-ą-vis civilian authorities in cyberspace, these are translated as literally as possible from the physical world. For example, the Dutch defence strategy for operating in cyberspace states that "[t]he three core tasks of the Defence organisation are leading for the armed forces' efforts in cyberspace."[9] When defining government responsibilities in cyberspace, states therefore generally start by adapting existing mandates and institutions.[10] Furthermore, there is general recognition of the need for a "comprehensive approach" to cyber security, in other words coordination between all stakeholders, and a need for cooperation between all relevant public, private and military entities. To improve cooperation, some countries like France and Australia have positioned the organization responsible for coordinating cyber policy at the highest level, directly under the prime minister or president. As ministries logically further their own organizational interests, be it the economy, human rights or security, this institutional construction allows for the balancing of higher order interests. An example would be defence or intelligence services advocating upstream data collection or keeping zero-day vulnerabilities unpatched for legitimate security reasons, while international economic or political repercussions might outweigh the security benefits.

Although the need for close cooperation between the armed forces and civilian authorities is often explicitly addressed in national security as well as national cyber security strategies, few countries are clear about the ways in which these intentions are to be realized. For instance, the French national cyber security strategy presents cyber defence as a civilian challenge, without mentioning the role of the armed forces.[11] Furthermore, although the armed forces are represented in the Information Systems Security Strategic Committee (*comité stratégique de la sécurité des systèmes d'information*), headed by the General Secretary for Defence and National Security, there is no further mention of the role the armed forces play in the response to high impact cyber attacks against critical infrastructure. Another example is the 2010 national security strategy of the United Kingdom which emphasises the "need [for] a whole-of-government approach to implementing this National Security Strategy."[12] Neither the national cyber security strategy nor the annual progress reports on the national security strategy and the national cyber security strategy, however, make any specific reference to cooperation between the armed forces and civilian cyber security authorities.

8 Thomas Rid & Ben Buchanan, '*Attributing Cyber Attacks*', Journal of Strategic Studies, Volume 38, Issue 1-2, 2015.

9 *The Defence Cyber Strategy*, Netherlands ministry of Defence, June 2012. Retrieved from: https://ccdcoe.org/strategies-policies.html [accessed March 2015].

10 Ian Wallace, '*Five Guiding Principles for the Development of National Cyber Strategies*', Brookings Opinion, June 2014.

11 *Information systems defence and security, France's strategy*, Office of the Prime Minister (2011), p. 21. Retrieved from http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf [accessed March 2015].

12 *A Strong Britain in an Age of Uncertainty: The National Security Strategy 2010*, p. 34. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf [accessed March 2015].

A common thread in Europe and several Asian countries is the limited role of the military in protecting critical infrastructure. This is understandable as most threats against national security in cyberspace will, at least during peace-time, be directed against civilian (public or private) infrastructure and will therefore have to be dealt with primarily by the organisations themselves, organisations responsible for sectoral oversight, and law enforcement agencies. Some nations have institutional and legal structures in place that allow for the assistance of the military in crisis management and incident response in case of a national emergency. In Europe, there seems to be consensus that these military capabilities should fall under civilian authority when deployed.[13] In many countries in Asia, however, a stronger and more coordinating role for the military does not seem controversial.[14] Nonetheless, in (cyber)crisis situations outside of an armed conflict, the role of the armed forces remains limited in most countries. National cyber security strategies indicate that in most countries the military have no formal responsibility at all, except in securing their own networks and as an eventual last resort if assistance is specifically requested by the civilian authorities. Japan seems to be the exception where paradoxically the armed forces have a very limited constitutional role. The Japanese National Cyber Security Strategy seems to give a leading role to the Self Defence forces in responding to cyber attacks against critical infrastructure, although the language is somewhat ambiguous.[15]

The emergence of a new policy area may lead to inter-agency fighting for as large a share as possible of newly allocated resources.[16] This can also take place within military organisations where there might be competition for resources between military intelligence and the various operational commands. Interagency rivalries can lead to unclear lines of command, often illustrated by the use of ambiguous language for the division of responsibilities. This vague use of language stands out when comparing national strategies and policy papers. In many countries, the division of responsibilities in crisis situations is not clear cut in official documents. Moreover, in situations where there is clear division of responsibilities, this has often not yet been tested in a real crisis situation. The current Dutch approach, for example, seems to be to bring together all the relevant stakeholders in a crisis situation and expect issues of command and responsibility to be resolved during the evolution of the crisis.[17]

However, in crisis situations, such vagueness will likely have a negative impact on the effectiveness of the response. The Estonian Cyber Security Strategy of 2014 recognises this problem and states that in order "to ensure the ability to provide national defence in cyberspace, the state's civilian and military resources must be able to be integrated into a functioning whole under the direction of civilian authorities as well as being interoperable with the capabilities of international partners."[18] Furthermore, to clarify such institutional issues and ensure that organisations are prepared when a crisis occurs, it is vital that nations conduct intensive training

13 Luijf e.a. '*Organisational structures & considerations*, in 'National Cyber Security Framework Manual', p. 121.

14 Authors' attendance at RSIS-Leiden University Centre for Terrorism and Counterterrorism (CTC) Roundtable on Civil-Military Relations in Cyberspace, Singapore, 18-19 November 2014.

15 Japan Cyber Security Strategy, 2013, p. 42; http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/JAP_NCSS2.pdf [accessed March 2015].

16 Luijf e.a, *Organisational structures and considerations*, in Klimburg e.a., 'National Cyber Security Framework Manual' (Tallinn 2012), p. 140.

17 Dennis Broeders, '*Investigating the Place and Role of the Armed Forces in Dutch Cyber Security Governance*', Department of Sociology, Erasmus University of Rotterdam, 2014, p.46.

18 *Estonian Cyber Security Strategy 2014-2017*, p 6; https://ccdcoe.org/strategies-policies.html [accessed March 2015].

and exercises with all stakeholders to get a more accurate understanding of the practical requirements in actual crisis situations.

Information-sharing between civilian and military or government and private actors is also considered to be crucial for crisis management and incident response. An important part of cyber defence, such as situation awareness, good threat intelligence analysis and building network resilience, takes place before the threat manifests itself as an attack. One institutional arrangement that facilitates information-sharing is the colocation of military and civilian Computer Emergency Response Teams (CERT's). This is, for instance, the case in France and Australia.[19] For example, the Australian Cyber Security Centre, which was established in November 2014, falls under the joint responsibility of the Attorney General and the Ministry of Defence. It is headed by a major general who commands the Department of Cyber and Information Security Directorate at Australia's Signals Intelligence Agency. It should be noted, however, that having a military officer as head of such a unit can convey a certain unwelcome signal to third (state) parties, in a region where military tensions should be carefully managed. Although certainly beneficial from an information sharing perspective, colocation could negatively impact on the perceived neutrality of government controlled CERT's.

When considering the role of the armed forces in cyber defence, it is important to also consider the distinction between the military and the intelligence sector. While the military often has a limited role in protecting national critical infrastructure outside of an armed conflict, the intelligence agencies play an increasingly important role in cyber security. In most countries, the technically proficient signals intelligence agencies have been tasked with cyber operations and these organisations are often military. The United Kingdom's Government Communications Headquarters (GCHQ) is one of the few signals agencies that is civilian and, in addition, also responsible for the government's CERT.[20] This is not an unusual construction and it allows for the efficient monitoring of networks for malware while also facilitating surveillance and espionage activities.[21] Intelligence agencies are responsible for the acquisition of data and information, and they execute covert operations that can encompass anything from sabotage to psychological operations.[22] This means accountability, transparency, and information-sharing with third parties are probably more complicated when intelligence organisations are involved instead of the military alone.

Regarding cooperation between (military) intelligence agencies and other public and private organisations, countries should recognise that the legitimate interests of these entities can vary greatly. For instance, the goal of a national CERT or a National Cyber Security Centre is to collect information on threats and vulnerabilities to inform stakeholders and provide solutions, whereas intelligence services may have a very different interest. They may instead require

19 In France, the Network and Information Security Agency (ANSSI), an overarching inter-ministerial authority that falls under the responsibility of the prime minister, hosts the CERT or crisis management centre (COSSI). This is co-located with a military CERT that is a part of the Defence cyber unit, the CALID, that is in turn part of the military cyber command. See http://www.ssi.gouv.fr/. For the institutional arrangement in Australia. See: http://www.asd.gov.au/infosec/acsc.htm [accessed March 2015].

20 See the official website at: http://www.cesg.gov.uk/AboutUs/Pages/aboutusindex.aspx [accessed March 2015].

21 While the military are bound by the internationally recognised legal cadres of humanitarian law, espionage is not constrained by any international legal framework.

22 Stuxnet is the prime example of a cyber (sabotage) operation conducted by state actors. See Kim Zetter, '*Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*', Crown Publishers, New York 2014.

information on threats and specific weaknesses so that they can exploit them when the national need arises. Cyber security strategies and policies therefore need to recognise and clearly define these different security interests.[23] The practice of designating an overarching responsible cyber unit facilitates an executive decision when these interests clash. National policies, regulations and procedures should stipulate what information should be shared, how organisations should work together to address a specific threat or incident, and how organisations should process and disseminate information on threats and vulnerabilities as well as counter measures.

3. ENHANCING MILITARY COOPERATION ACROSS ASIA AND EUROPE

The challenges faced by nations when defining the role of the military regarding cyber security also have important international dimensions. Improving international cooperation between civilian and military entities and between international organisations should therefore strengthen the national security of individual states. This section therefore considers structures across Asia and the EU to enable better international military cooperation between the two regions for cyber related incidents. Given the widespread concern that a cyber incident, whether in the civilian or military domains, could cause tensions and unwanted escalation, makes efforts to improve international cooperation especially important. Additional mechanisms should be developed to enhance transparency, predictability, and stability and to reduce the risks of misperception, escalation, and conflict that may stem from the use of cyber capabilities.[24] This is especially the case since military cooperation structures are currently at a relatively early stage of development. In terms of establishing cooperation, it is also important to consider that, as noted earlier, not all countries across these two regions share the same threat perception or strategic priorities. Historical context, domestic considerations and the wider geostrategic context in both regions remain significant factors. And while several of these findings may not be particularly surprising, with the requisite political willingness, there are several mutually beneficial opportunities for deeper cooperation that could be pursued as a starting point for longer term collaboration.

Improved mechanisms are important given (i) the nature of cyber threats; (ii) the growing interest in cyber capabilities that are difficult to control with arms control mechanisms; (iii) an increasing recognition by many states of cyber as another domain for military operations, and (iv) operations that are becoming increasingly dependent on the availability of a secure digital environment. While there is a great deal of institutional capacity within NATO and the EU, experts highlight that beyond this there is a lack of fixed structure or templates for international military cooperation. At this juncture, military-to-military cooperation on cyber related matters is somewhat limited, particularly since countries are at different stages of policy development, and common understanding (which experts cite as one of the most important factors for cooperation) is lacking in this area.[25] The EU Cyber Defence Policy Framework, which was adopted in November 2014, identifies the significance of international cooperation and states that there is a need to ensure dialogue with international partners, specifically NATO and other

23 For the perils of informal information-sharing arrangements, see Ewen MacAskill, 'Ex MI6 Chief calls for new compact between internet firms and spy agencies', The Guardian, 20 January 2015.

24 OSCE participating states in Permanent Council Decision No. 1039 decided to elaborate a set of draft CBMs to enhance interstate cooperation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs.

25 Authors' attendance, RSIS-Leiden CTC Roundtable.

international organisations (in particular, it states that increased engagement should be sought within the framework of the OSCE and UN).[26] The European Defence Agency (EDA) and European External Action Service (EEAS) are therefore establishing a more extensive contact network and beginning to engage both at the bilateral level with third countries in Asia, such as India and China for example, as well as with regional organisations.[27] The 2013 Cyber Security Strategy of the EU also calls for increased engagement with key international partners and organisations and recommends that EU consultations should be designed and coordinated to add value to existing bilateral dialogues between EU Member states and third countries.[28]

This is especially significant for the Asia region, where interstate relations are complex. When considering European policies toward Asia, it is important to not just consider the role of the EU collectively but also EU Member states' national strategies and the complex relationship between the two.[29] Furthermore, general observations point out that while EU Member states "tend to break ranks in pursuit of national gain" across the world, the "multilevel complexity of relations between Europe and Asia is of a different order to the situations that exists in other regions".[30] Analysts highlight what seems to be a growing view in ASEAN that the EU has become overly anxious over China's rise and is consequently still neglecting to engage systematically with the rise of other Asian powers.[31] In Asia, ASEAN is central in a regional architecture that includes groupings such as the ASEAN Regional Forum (ARF), ASEAN +3, East Asia Summit, and the ASEAN Defence Ministers Meeting-Plus (ADMM-Plus). The ADMM and ADMM-Plus are the key defence forums within ASEAN that focus deliberately on practical cooperation. The ARF provides an important opportunity for dialogue and it has hosted several workshops on matters such as the use of proxy actors, cyber incident responses, and CBMs in cyberspace. A working draft on CBMs is under negotiation by ARF participants, including the EU, and it is hoped that an active contact list will be agreed soon. However, there is some criticism that this process has already taken over two years.[32] Furthermore, experts have voiced concern over the efficiency of such diplomatic channels in this region given the speed with which cyber incidents might occur and the fact that there can be some difficulty in establishing what falls within either the political or military realms.[33] For now, there does not seem to be extensive coordination between the dialogue at the ARF and the ADMM and, ideally, the work of the foreign affairs tracks on cyber related matters could complement that of defence.

While several statements calling for regional collaboration on cyber threats have been issued by defence ministers at previous ADMM meetings, discussions on stronger collaboration and the possible development of an "ASEAN master plan of security connectivity" do not seem to have extensively progressed.[34] The Network of ASEAN Defence and Security Institutions (NADI)

26 Council of the European Union, EU Cyber Defence Policy Framework, 15585/14, 18 November 2014, p. 2. See also: related General Affairs Council conclusions, 25 June 2013.
27 Neil Robinson, "EU cyber defence: a work in progress", European Union Institute for Security Studies, Brief Issue 10, March 2014, p. 4.
28 Joint communication, *Cybersecurity Strategy of the European Union*, p. 15.
29 Richard Youngs, "*Keeping EU-Asia Reengagement on Track*", Carnegie Europe, January 2015, p. 4.
30 Ibid.
31 Ibid.
32 Authors' attendance, RSIS-Leiden CTC Roundtable.
33 Ibid.
34 *"ASEAN must tackle cyber security threat"*, New Straits Times, 31 May 2012. See also: IISS, *"New Forms Of Warfare - Cyber, UAV's and Emerging Threats: Dato'* Seri Dr Ahmad Zahid Hamidi", http://www.iiss.org/en/events/shangri%20la%20dialogue/archive/sld12-43d9/fourth-plenary-session-1353/dato-seri-dr-ahmad-zahid-hamidi-b13b [accessed March 2015].

did hold a workshop on emerging cyber security challenges and responses in 2013 at which it tabled recommendations for consideration. NADI is a Track II forum that complements the ADMM and furnishes recommendations into the ADMM process by bringing defence officials and analysts together to discuss security matters that are sometimes deemed too sensitive for discussion at official Track I meetings.[35] While there is a close network of officials who regularly attend the ASEAN defence meetings and an evident shared focus on the concrete implementation of policies that rivals parallel negotiations between civilian ministries, there is still a greater need in both the ASEAN region and the wider Asia Pacific for enhanced CBMs and transparency measures such as further military-to-military engagements, dialogue, information sharing, joint exercises, official military-to-military contact points, and crisis communication procedures.

In both the EU and Asia, cyber defence is a national sovereign prerogative. Military cyber defence in the EU is currently considered to be at a relatively early stage of maturity.[36] Moreover, cyber defence capability varies greatly between the Member states - for example, a 2013 EDA-commissioned study found a complex and diverse picture regarding cyber defence capabilities within the 20 participating Member states.[37] The study further noted that the complex operational set up between the EDA, EEAS, General Secretariat of the EU Council and European Commission, and related EU agencies like the European Network and Information Security Agency (ENISA), the European Cybercrime Centre (EC3) and CERT-EU should be highlighted.[38]

Similarly, the Asia Pacific is a diverse region comprising countries that are at very different stages in terms of cyber technologies as well as strategy development and implementation. In addition, the institutional and operational structures of regional organisations, like the much smaller ASEAN Secretariat, are far more simplistic than those within the EU. Cyber defence capabilities vary significantly between countries across the region and given the sensitivities surrounding cyber security, in particular capabilities, it can be difficult to precisely ascertain the extent to which state actors have developed or acquired capabilities. In spite of this, increased military developments of operational cyber capabilities are expected.[39] The challenge lies not so much in an increase in military acquisition of capabilities, since states will seek to develop capabilities, but rather experts are also concerned about the current lack of military-to-military dialogue.[40] This is particularly pertinent given the strategic context of the Asia Pacific region where there are high national security sensitivities, unprecedented military modernisation and defence spending, on-going territorial and maritime disputes, uncertainty surrounding China as a regional military power and the United States' *'pivot'* towards Asia, as well as heightened concerns over North Korea. Non-state actors cause even further complication, and the growing

35 Track II diplomacy generally refers to non-governmental, informal and unofficial contact and activities that can assist official actors by exploring solutions without the requirements of formal negotiation whereas Track I diplomacy can be defined as official, governmental diplomacy.

36 European Defence Agency, "*Cyber Defence Fact Sheet*", www.eda.europea.eu [accessed March 2015].

37 Ibid. EDA has 27 participating member states (all EU with exception of Denmark).

38 Ibid. In general, EEAS leads third party (state or organisation) dialogues and cooperation. Although the EUMS and EDA have their own authorities to establish links with third parties, this is much more limited.

39 Australian Strategic Policy Institute, "*Cyber Maturity in the Asia-Pacific Region 2014*", ASPI International Cyber Policy Centre, April 2014, p. 7.

40 Authors' attendance, RSIS-Leiden CTC Roundtable.

levels of cybercrime in the region could cause further instability because of connections to espionage and military activities.[41]

In fact, current analyses identify that the most dynamic areas of Europe-Asia relations have recently come through extended bilateral efforts on both sides rather than on a region-to-region basis.[42] Such bilateral cooperation could be less problematic for militaries to develop, particularly since it might sometimes be easier to establish trust and when the relationship is based on national priorities, shared interests are often easier to identify.[43] In order to create an environment for cooperation in cyber defence, military experts argue that while these are sovereign decisions, sovereignty itself is not in fact the decisive factor - trust and shared interests are more powerful drivers when deciding on the degree of cooperation.[44] More recently, analysts further observe that cooperation efforts at the sub-regional level between like-minded groupings from Asia and Europe can sometimes allow for the embedding of practices that could then be extended to a regional level.[45] These observations also apply to cooperation efforts between groupings in Asia and Europe (or further afield) in cyber related matters. Although, some argue that while it is probable that like-minded communities can create CBM's and transparency mechanisms more easily, they are pessimistic when it comes to potential adversaries given, for instance, the visible difficulties of establishing such mechanisms in the U.S.-China working group.[46] Given these realities, states from Asia and Europe should concentrate on building better trust and coordinated cooperation at bilateral and regional levels that are mutually reinforcing.

Several additional mechanisms could be considered to enhance cooperation between Europe and the Asia Pacific region. For instance, Track I and Track II consultations and workshops can provide a venue for the exchange of opinions, military doctrine and strategies, national structures and best practice in crisis management or civilian missions. Such exchanges can enhance transparency and communication in order to build trust and common understanding as well as create informal networks and contact points. More particularly, if meetings were to be held more regularly, this would again allow for more enhanced trust and common understanding. For example, ARF participants took part in a table-top exercise in March 2014 to exchange details on national practices, and a roundtable on civil-military relations in cyberspace in November 2014 allowed for exchange of opinions and national strategies while also informally gathering a network of defence officials from across Asia and Europe.[47]

While multilateral MOUs could also be considered, Asian officials further suggest that international security and defence forums like, for instance, the Shangri-La and Seoul Defence dialogues, are helpful mechanisms to engage in dialogue on cyber defence.[48] At the Seoul

41 James Lewis, "*Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia*", prepared for the Lowy Institute MacArthur Asia Security Project, 2013, http://csis.org/files/publication/130307_cyber_Lowy.pdf, [accessed March 2015].
42 Youngs, "Keeping EU-Asia Reengagement on Track", p. 7.
43 Authors' attendance, RSIS-Leiden CTC Roundtable.
44 Wolfgang Röhrig and Wg. Cdr. Rob Smeaton, "*Cyber Security and Cyber Defence in the European Union*", https://www.eda.europa.eu/docs/default-source/documents/23-27-wolfgang-r%C3%B6hrig-and-j-p-r-smeaton-article.pdf, [accessed March 2015].
45 Youngs, "Keeping EU-Asia Reengagement on Track", 19.
46 Authors' attendance, RSIS-Leiden CTC Roundtable.
47 ARF Workshop on Cyber CBMs, Kuala Lumpur, March 2014 & RSIS-Leiden CTC Roundtable, Singapore, November 2014.
48 Authors' attendance, RSIS-Leiden CTC Roundtable.

Defence Dialogue in 2014, for example, over 20 countries discussed the military's role in cyber and a working group was established to promote pragmatic dialogue in order to enhance common understanding and ultimately, to assist in establishing structures for cooperation.[49] Singapore's Defence Minister recently echoed similar sentiments when urging enhanced collaboration through multilateral platforms like the Shangri-La Dialogue and ADMM-Plus grouping.[50]

The Multinational Capability Development Campaign (MCDC) has also been proffered as an opportunity for engagement since, although it is led by the U.S., it is regarded as a neutral platform operating at the unclassified level with less political constraints (Japan and South Korea are observers for example).[51]

Identifying and retaining cyber experts in the armed forces is also identified as a common problem in both the EU and across several countries in Asia, especially since this is a competitive market given the more profitable civilian domains. This is another area where collaborative exercises or discussions on best practices could be exchanged. In fact, the EU Cyber Security Strategy of 2013 suggests the EDA and Member states should collaborate on improving cyber defence training and exercise opportunities in the European and multinational context. The EU Cyber Defence Policy Framework further proposes the establishment of a cyber defence dialogue on training standards and certification with third countries and international organisations.[52] At national level, a number of states have been running bilateral or small exercises with other like-minded nations.[53]

4. CONCLUSION

Due to differing threat perceptions and a large diversity of political systems and cultures across Asia and Europe, the institutional embedding of roles and responsibilities in the cyber domain is generally based on specific national political and organizational traditions and processes. Consequently, there is no single institutional construction that can be identified as a model for others. Although countries recognise that the government shares responsibility for the protection of critical infrastructure against cyber threats, in most cases the military only play a limited role. Often the exact roles that different ministries and the military should play during crisis and incident response are not clearly formulated in the cyber strategy and policy documents. In so far as there are clear institutional arrangements, these are generally still untested given that (actual) cyber crises involving critical infrastructure in Europa and Asia have been have as of yet only occurred sporadically. Carrying out exercises would certainly contribute to the clarification of the roles of different stakeholders.

Civil-military relations can be improved through different mechanisms. Clearly defined procedures facilitate information-sharing between different parties and stakeholders. The exact

49 Seoul Defense Dialogue 2014, http://sdd.mnd.go.kr/user/boardList.action?boardId=O_63480&siteId=sdd&page=1&search=&column=&boardType=02&listType=&id=sdd_060300000000&parent=&boardSeq=O_63492&command=albumView&chkBoxSeq=&chkBoxId=&chkBoxPos=&chkBoxDepth=&chkBoxFamSeq=&warningYn=N&categoryId=&categoryDepth=.

50 Jermyn Chow, "*Ng Eng Hen: Deeper issues beyond the ISIS threat*", Straits Times, 27 January 2015.

51 Authors' attendance, RSIS-Leiden CTC Roundtable.

52 *EU Cyber Defence Policy Framework*, p. 11.

53 Röhrig and Smeaton, "*Cyber Security and Cyber Defence*".

role and responsibility of the intelligence agency in the national cyber landscape is crucial in many countries and will determine how information is shared between public and private actors, as well as how networks of trust and questions relating to transparency can be addressed. States must be aware that all institutional arrangements, such as military commanders for civilian cyber centres, as well as the wording of their cyber security strategies, not only serve a national purpose but also have a strong declaratory function vis-a-vis other state parties.

Given the international nature of the cyber threat, it is not only important to improve mechanisms for dialogue, cooperation, and transparency within regional structures such as the EU and ASEAN but also between the two regions. States from Asia and Europe should therefore concentrate on building better trust and coordinated cooperation, where appropriate, at bilateral and regional levels that is mutually reinforcing. Moreover, in situations where interstate tensions are prevalent, improved military-to-military communication is vital. In this regard international meetings, like the civil-military Singapore roundtable, held in November 2014 are useful to build trust and create understanding between different policy makers.