ENABLING BETTER MULTINATIONAL AND INTERNATIONAL MILITARY COOPERATION FOR CYBER-RELATED MATTERS ACROSS ASIA AND EUROPE

Policy Report
March 2015

Caitríona H. Heinl

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Policy Report

ENABLING BETTER MULTINATIONAL AND INTERNATIONAL MILITARY COOPERATION FOR CYBER-RELATED MATTERS ACROSS ASIA AND EUROPE

Caitríona H. Heinl
March 2015

Centre of Excellence for National Security (CENS),
S. Rajaratnam School of International Studies (RSIS),
Nanyang Technological University (NTU)

Executive Summary

This brief considers the structures in place across Asia and the European Union (EU) to enable better international military cooperation for cyber-related incidents. Improved mechanisms for international military cooperation are important given (i) the nature of cyber threats; (ii) the growing interest in cyber capabilities that are inherently difficult to control with arms control mechanisms; and (iii) an increasing recognition by many states of cyber as another domain for military operations. Moreover, operations are becoming increasingly dependent on the availability of a secure digital environment. However, cooperation structures are at a relatively early stage of development and they are still evolving.

This brief therefore outlines how international cooperation — including confidence-building measures (CBMs) — might assist a better exchange of information over the near to medium future to increase cyber defence effectiveness as well as enhanced stability. Lastly, it identifies several best practices and possible opportunities for further cooperation, specifically between Asia and Europe.

Introduction

While cyber-related activities will most likely play a part in most future conflicts, at the moment there is often a limited understanding of the nature of cyber attacks and their possible impact, in addition to a dearth of knowledge about the intentions of possible opponents and difficulties in attribution. Subsequently, there is widespread concern that a cyber incident could cause tensions to escalate far too quickly, which makes efforts to improve international cooperation especially important. More mechanisms should be further developed to enhance transparency, predictability, and stability and to reduce the risks of misperception, escalation, and conflict that may stem from the use of these capacities.[1] This is particularly the case given the unique nature of cyber threats, growing military interest in cyber capabilities that are difficult to control with arms control mechanisms, as well as the rising recognition by many states of cyber as a domain for military operations. Operations are also becoming increasingly dependent on the availability of a secure digital environment.

Analysts in both the EU and Asia have observed that many countries are still grappling with the conceptual and doctrinal underpinnings of the role of military and armed forces in defending cyberspace, albeit to different degrees.[2] However, although these structures are still under development within both regions, it is also important to consider that not all countries share the same threat perception or strategic priorities. Historical context, domestic considerations and the wider geostrategic context in both regions are significant factors that should be borne in mind.

While there are some examples of cooperation between the two regions, such cooperation mechanisms are still developing. Currently, although there is a great deal of structure within the North Atlantic Treaty Organization (NATO) and the EU, practitioners highlight that beyond this there is a lack of fixed structure or templates for international military cooperation.[3] At this juncture, military-to-military cooperation for cyber-related matters is somewhat limited, particularly since countries are at different stages of development, and common understanding (which practitioners cite as one of the most important factors for cooperation) is lacking.[4]

One of the five priorities of the 2013 Cybersecurity Strategy of the EU is the development of cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP) framework.[5] Pursuant to this strategy, the EU Cyber Defence Policy Framework was adopted by the Council of the European Union in November 2014.[6] Among other priorities, this framework identifies the significance of international cooperation and states that there is a need to ensure a dialogue

---

1 OSCE participating states in Permanent Council Decision No. 1039 decided to elaborate a set of draft confidence building measures 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.

2 Neil Robinson, "EU cyber-defence: a work in progress", European Union Institute for Security Studies, Brief Issue 10, March 2014, 2.

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

4 Ibid

5 Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final, 7 February 2013, 5. See also: Wolfgang Roehrig & JPR Smeaton, "Viewpoints: Cyber Security and Cyber Defence in the European Union", https://www.eda.europa.eu/info-hub/opinion/2014/06/11/viewpoints-cyber-security-and-cyber-defence-in-the-european-union, European Defence Agency Opinion, 11 June 2014.

6 Council of the European Union, *EU Cyber Defence Policy Framework*, 15585/14, 18 November 2014, 2. Note: On the basis of a proposal by the High Representative in cooperation with the European Commission and EDA. See also: related General Affairs Council conclusions of 25 June 2013.

with international partners, specifically NATO and other international organisations, in order to contribute to the development of effective cyber defence capabilities.

In particular, the EU Cyber Defence Policy Framework states that increased engagement should be sought within the framework of the OSCE and UN. The 2013 Cybersecurity Strategy of the EU also calls for cyberspace issues to be integrated into EU external relations and its Common Foreign and Security Policy (CFSP) in order to increase engagement and stronger relations with key international partners and organisations (as well as civil society and the private sector).[7] It further recommends that EU consultations on cyber issues should be designed and coordinated to add value to existing bilateral dialogues between EU Member States and third countries.[8] This is especially significant for the Asia region. 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.[9] These considerations also apply to EU aims, highlighted under the 2013 Cybersecurity Strategy, to seek closer cooperation with international organisations such as ASEAN. 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).

Representatives from the EU were present at the last ARF workshop on cyber CBMs in March 2014.[10] The ARF provides an important opportunity for open dialogue, in particular among three of the most advanced global cyber actors – the United States, Russia, and China.[11] This forum has hosted a number of workshops on cybersecurity matters such as the use of proxy actors, cyber incident responses, and CBMs in cyberspace. It also has a working draft on CBMs that is currently under negotiation by ARF participants, including the EU, and it is hoped that an active contact list will be soon agreed. Nevertheless, there is some criticism that this process has already taken over two years and it should not be this difficult to agree on active points of contact.[12] Given the unique membership of the ARF however, this might provide some explanation as to why the process has been this lengthy. The announcement at an EU-ASEAN meeting in July 2014 of the EU's intention to appoint an Ambassador to ASEAN and to grant the association the status of strategic partner might also assist future negotiations in that it will ensure a more regular presence.[13]

However, there is some further concern from practitioners over the efficiency of such diplomatic channels 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.[14] For now, there does not seem to be extensive coordination between the dialogue at the ARF and the ADMM yet. The ADMM and ADMM-Plus are the key defence forums within ASEAN that focus deliberately on practical cooperation. Ideally, the work of the foreign affairs tracks on cyber-related matters could complement that of defence.

---

7 Joint communication, *Cybersecurity Strategy of the European Union*, 15.

8 Ibid

9 Richard Youngs, "Keeping EU-Asia Reengagement on Track", Carnegie Europe, January 2015, 4.

10 Author's attendance at the ASEAN Regional Forum Workshop on Cyber Confidence Building Measures, Kuala Lumpur, 25-26 March 2014.

11 Caitríona Heinl, "Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime", *Asia Policy*, Number 18, The National Bureau of Asian Research, July 2014, 131-59.

12 Author's attendance at RSIS-Leiden University CTC Roundtable on Civil-Military Relations.

13 Youngs, "Keeping EU-Asia Reengagement on Track", 14.

14 Author's attendance at RSIS-Leiden University CTC Roundtable on Civil-Military Relations.

Regarding other international organisations and relevant EU international partners, the European External Action Service (EEAS) and the European Defence Agency (EDA), with the Member States, outline three points of action in the EU Cyber Defence Policy Framework. First, they will follow strategic developments and hold consultations in cyber defence issues with partners such as international organisations and third countries. Second, they will explore possibilities for cooperation on cyber defence issues, including with third countries participating in CSDP missions and operations, and third, they will continue to support the development of CBMs in cybersecurity, to increase transparency and reduce the risk of misperceptions in state behaviour by promoting the on-going establishment of international norms in this field.[15] The EDA and EEAS are therefore establishing contacts 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.[16] In general, the EEAS leads all third party (state or organisation) dialogues and cooperation.[17]

At this point in time, military cyber defence in the EU is considered to be at a relatively early stage of maturity.[18] Nor does the EU have standing military forces or EU-owned military equipment so that when it launches a military operation, it is dependent on force contributions from its Member States or other force contributors.[19] In other words, military force generation and readiness are a national rather than EU competence.[20] Cyber defence in both the EU and Asia is therefore a national sovereign prerogative.

Cyber defence capability also varies greatly between EU Member States. Defence officials consequently argue that they must all now invest and continue to invest in cyber defence capabilities.[21] For example, a 2013 study commissioned by the EDA to better understand cyber defence capabilities across EDA participating Member States, in order to support progress towards a more consistent level of cyber defence capability across the EU, found a complex and diverse picture with regard to cyber defence capabilities within the 20 participating Member States.[22] The study further noted that when considering cyber defence among EU organisations 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.[23]

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. Although 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 greatly between countries across the Asia Pacific. Moreover, given the current sensitivities surrounding cybersecurity, in particular cyber capabilities, it can often be difficult to precisely ascertain the extent to which state actors in the region have developed or acquired capabilities. In spite of this, increased military developments

---

15 On matters of international security, the EU encourages the development of CBMs in cybersecurity, to increase transparency and reduce the risk of misperceptions in state behaviour. See: Joint communication, *Cybersecurity Strategy of the European Union*, 15.

16 Robinson, "EU cyber-defence", 4.

17 Although the EUMS and EDA have their own authorities to establish links with third parties this is much more limited.

18 European Defence Agency, "Cyber Defence Fact Sheet", www.eda.europea.eu, last updated 24 March 2014, 2.

19 Roehrig & Smeaton, "Cyber Security and Cyber Defence".

20 Robinson, "EU cyber-defence", 2.

21 Roehrig & Smeaton, "Cyber Security and Cyber Defence".

22 European Defence Agency, "Cyber Defence Fact Sheet", 1. EDA has 27 participating Member States (all EU MS with the exception of Denmark).

23 Ibid

of operational cyber capabilities are expected.[24] The difficulty though, is not so much the visible increase in the acquisition of military capabilities, since states will always seek to develop capabilities, but rather practitioners are also concerned about the current lack of military-to-military dialogue.[25] 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. And non-state actors such as cyber criminals, terrorists, hackers, hacktivists, and proxy actors engaged or supported by government, cause even further complication. This is especially the case since growing cybercrime in the region could cause further instability because of its connections to espionage and military activities.[26]

While a number of statements calling for regional collaboration to deal specifically with cyber threats have been issued by defence ministers in Southeast Asia at previous ADMM meetings, discussions on stronger collaboration in cyber defence and the possible development of an "ASEAN master plan of security connectivity" do not seem to have progressed any further.[27] The Network of ASEAN Defence and Security Institutions (NADI) also held a workshop on emerging cybersecurity challenges and responses in 2013. NADI is a Track II forum that complements the ADMM and furnishes recommendations into the ADMM process. It brings defence officials and analysts together to discuss security matters that are sometimes deemed too sensitive for discussion at official Track I meetings.

Although there is a close network of officials who regularly attend these ASEAN meetings, there is still, without doubt, 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 to help prevent miscalculations, misunderstandings, false attribution or escalation in tensions. In fact, military-to-military relations can sometimes be simpler to establish given common hierarchies, terminologies, and structures that often transcend national differences. This is especially evident when it comes to a shared focus on the concrete implementation of policies, which can sometimes even rival parallel negotiations between civilian ministries.

While developing further forms of international cooperation, the inherent difficulties surrounding the current sensitivities of these cyber defence matters must also be taken into account. Although, some officials note that there might be a danger of overstating the importance of the military given that most threats are often criminal in nature.[28] Furthermore, there is still some debate that requires further analysis as to whether most countries would still prefer to work on their national positions internally before engaging regionally and internationally or whether regional and international cooperation efforts could instead assist national efforts.[29]

---

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

25 Author's attendance at RSIS-Leiden University CTC Roundtable on Civil-Military Relations.

26 James Lewis, "Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia", http://csis.org/files/publication/130307_cyber_Lowy.pdf, prepared for the Lowy Institute MacArthur Asia Security Project, 7 March 2013.

27 New Straits Times, "ASEAN must tackle cyber security threat", http://news.asiaone.com/News/Latest+News/Science+and+Tech/Story/A1Story20120531-349622.html, 31 May 2012.

28 See also: IISS, "New Forms Of Warfare - Cyber, UAVs 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, Shangri-La Dialogue, 03 June 2012.

28 Author's attendance at RSIS-Leiden University CTC Roundtable on Civil-Military Relations.

29 Ibid

Although there is a clear need for de-escalation mechanisms, some practitioners argue that while it is probable that like-minded communities can create these 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.[30]

Bilateral discussions are also being held among some countries in the Asia Pacific region including over the possible establishing of hotlines like the China-Japan hotline (although there could be a danger in having too many hotlines).[31] In order to create an environment for cooperation in cyber defence, defence 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.[32] Consequently, bilateral cooperation could be less problematic for militaries to develop, particularly since it might sometimes be easier to establish trust.[33]

Because the relationship is based on national priorities, shared interests are often easier to identify.[34] Alternatively, cooperation efforts at the sub-regional level between like-minded groupings from Asia and Europe could also allow for the embedding of practices that could then be extended to a regional level.[35] 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.[36] Consequently, Europe-Asia relations are now "a diffuse patchwork of national, subregional, and regional initiatives that sometimes reinforce but often cut across eachother".[37] 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".[38] Lastly, there 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.[39] Given these realities, states from Asia and Europe should do their utmost to build trust and cooperation at bilateral and regional levels that is mutually reinforcing.

Further Mechanisms for Deeper Cooperation between Europe and the Asia Pacific

In addition to 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, this section provides several observations on additional mechanisms that could be considered to enhance cooperation between Europe and the Asia Pacific region.

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

---

30 Ibid

31 Ibid

32 Roehrig & Smeaton, "Cyber Security and Cyber Defence".

33 Author's attendance at RSIS-Leiden University CTC Roundtable on Civil-Military Relations.

34 Ibid

35 Youngs, "Keeping EU-Asia Reengagement on Track", 19.

36 Ibid, 7.

37 Ibid

38 Ibid

39 Ibid

informal networks and contact points. More particularly, if meetings were to be held more regularly, this would also allow for more enhanced trust between parties. By way of example, ARF participants took part in a table-top exercise at the forum's workshop on CBMs in March 2014 to exchange details on national practices, and a roundtable on civil-military relations in cyberspace in November 2014 allowed for an exchange of opinions and national strategies while also informally gathering a network of defence officials from across Asia and Europe.[40]

While multilateral MOUs could also be considered, Asian officials also suggest that international security and defence forums, like both the Shangri-La and Seoul Defence dialogues for instance, are helpful mechanisms to engage in dialogue on cyber defence matters.[41] At the Seoul Defence Dialogue, 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.[42] Singapore Defence Minister Ng Eng Hen recently echoed similar sentiments when urging enhanced collaboration among countries through multilateral platforms like the Shangri-La Dialogue and ADMM-Plus grouping, particularly since such practical cooperation can build confidence and mutual understanding as well as help prevent incidents from spiralling out of control on account of misunderstandings or miscalculations.[43]

The Multinational Capability Development Campaign (MCDC) has also been proffered as an opportunity for engagement for any nation since, although it is led by the United States, it is still regarded as a neutral platform that operates at the unclassified level with less political constraints (Japan and South Korea are observers for example).[44]

Operational cooperation between national computer emergency response teams (CERTS) has often been informal and somewhat easier to achieve. In particular, in crisis situations, cooperation at CERT-to-CERT level can prove invaluable. This is an area where cooperation could be enhanced by facilitating inter-regional information sharing and real-time responses to cyber incidents as well as strengthening existing operational cooperation with regional and international response teams such as the Asia Pacific Computer Emergency Response Team (APCERT), CERT-EU or the relevant EU cyber defence bodies, FIRST, and possibly the NATO Computer Incident Response Capability (NCIRC). NATO malware information sharing platforms/databases could also be considered as a possible form of technical cooperation.[45]

Growing and retaining cyber-trained people 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 to both train and retain skilled individuals could be exchanged. In fact, the EU Cybersecurity Strategy of 2013 highlighted that the High Representative would invite the EDA and Member States to collaborate on improving cyber defence training and exercise opportunities for the military in the European and multinational context. In November 2012, the EU defence ministers placed cyber defence on the pooling and sharing agenda and the

---

40 Author's attendance at ARF Workshop on Cyber Confidence Building Measures & RSIS-Leiden University CTC Roundtable on Civil-Military Relations.

41 Author's attendance at RSIS-Leiden University CTC Roundtable on Civil-Military Relations.

42 Ibid

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

44 Author's attendance at RSIS-Leiden University CTC Roundtable on Civil-Military Relations.

45 Ibid

EDA consequently established a framework for "achieving more without losing sovereignty over assets and resources" with projects in cyber defence training and exercise ranges (further options are under evaluation).[46] 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.[47]

EU-level organisations like the European Security and Defence College (ESDC) run general training courses on cyber defence, and other actors in the civil or law enforcement domain such as ENISA or the European Cybercrime Training and Educations Group (ECTEG) produce technical and operational training products as well as a variety of courses.[48] ENISA has also been responsible for organising cybersecurity exercises such as the pan-European Cyber-Europe 2014 exercise.[49] In addition, the EU Cyber Defence Policy Framework suggests that the possibility of participation in other multinational cyber defence exercises should be considered.[50] At national level, a number of states have been running bilateral or small exercises with other like-minded nations.[51] The training of decision-makers is another opportunity for collaboration, and the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), for instance, runs such courses for decision-makers.

To conclude, there is a growing interest in pursuing further international military cooperation between state actors across Asia and Europe for cyber-related matters. Given the unique nature of cyber threats, such transparency and military-to-military communication is vital, especially in situations where interstate tensions are prevalent. While the mechanisms that are currently in place are at an early stage of development, with the requisite political willingness, there are several mutually beneficial opportunities for deeper cooperation that could be pursued.

---

46 Roehrig & Smeaton, "Cyber Security and Cyber Defence".

47 Council of the European Union, *EU Cyber Defence Policy Framework*, 11.

48 Roehrig & Smeaton, "Cyber Security and Cyber Defence".

49 Ibid

50 Council of the European Union, *EU Cyber Defence Policy Framework*, 12.

51 Roehrig & Smeaton, "Cyber Security and Cyber Defence".

About the Author

Caitríona H. Heinl is a Research Fellow responsible for research on cybersecurity matters under the Homeland Defence Programme at the Centre of Excellence for National Security (CENS) within the S. Rajaratnam School of International Studies (RSIS). CENS is a research unit which works closely with the National Security Coordination Secretariat (NSCS) within the Prime Minister's Office, Singapore.

Sergei Boeke, Research Fellow, International Centre for Counter-Terrorism, Leiden University, contributed to this policy report.

About the Centre of Excellence for National Security

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, Singapore.

Established on 1 April 2006, CENS *raison d'être* is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues.

CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs. Besides fulltime analysts, CENS further boosts its research capacity and keeps abreast of cutting edge global trends in national security research by maintaining and encouraging a steady stream of Visiting Fellows.

About the S. Rajaratnam School of International Studies

The **S. Rajaratnam School of International Studies (RSIS)** is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS' mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-Traditional Security, International Political Economy, and Country and Region Studies. RSIS' activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information about RSIS, please visit **www.rsis.edu.sg**.

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg