The Role of the Military in Cyber Space: Civil-Military Relations and International Military Co-operation

by **Ms Caitríona Heinl**

Abstract:

This article highlights the significance of co-ordination that is key at both the national level within a state and between countries from a strategic and policy perspective for cyber-related issues. It first considers several significant matters that arise in terms of the role of the military and civil-military co-ordination for cyber security. It also highlights a number of challenges in finding the right roles and responsibilities for the military in national cyber security. The article then focuses on military co-operation and dialogue. Finally, it analyses how to ensure that there are mechanisms to prevent further escalation when militaries are involved in managing these threats.

Keywords: Cyber security; Civil-military Relations; Trust; Military Co-operation and Dialogue; Transparency

IMPROVING CIVIL-MILITARY CO-ORDINATION IN CYBER SECURITY[1]

Several important issues can arise for countries in terms of civil-military co-ordination for cyber security, and this accentuates the significance of co-ordination between various agencies within a state. This section will highlight a number of challenges that can arise in finding the right roles and responsibilities for the military in national cyber security. It does so in general terms by identifying common challenges for many countries rather than by providing a country-specific analysis of military strategic approaches. These models can range from countries that adopt a closely integrated civil and military approach, like the Scandinavian countries, to the other extreme where countries adopt a looser co-ordination between the civil and military sectors, such as Germany.[2]

The nature of cyber-related developments has been increasingly affecting traditional civil-military relations to the extent that militaries must consider a number of implications. For instance, (1) cyber capabilities are by nature inherently difficult to verify through arms control mechanisms; (2) the nature of cyber-related threats means that there can be a grey area between criminal and malicious state activity; (3) capabilities are dual-use; and (4) the role of the private sector is crucial. Consequently, several challenges that have arisen for many states include, among others: (1) how to embed cyber security in a nation's public institutions; (2) how to better clarify the exact role of the military; (3) the need for enhanced information-sharing; (4) how to build trust; and (5) managing limited financial and labour resources.

Decision-Making

Cyber-related matters often fall under the purview of several government ministries, and consequently many countries have been working out how to embed cyber security in public institutions over the past

few years in order to ensure that responsibilities are clearly defined, bureaucratic stovepipes avoided and co-operation maximised.

For example, several countries have positioned the entity responsible for co-ordinating cyber policy at the highest level like the office of the prime minister or president. One explanation for this is that although military or intelligence services may act in accordance with their own organisational interests, by raising decision-making to such higher levels, interests might then be balanced. These interests include weighing the impact of security policies on the economy and international relations, or weighing the proportionate balance between security and privacy or civil liberty issues.[3]

Better Clarification Of The Role Of The Military

While tensions regarding military involvement in cyber space may arise, the military is a significant stakeholder with an interest in a safe and secure cyber space. Moreover, an increasing number of states are recognising cyber space as a domain for military operations. Nevertheless, while many are currently refining their national cyber security strategies, the military's exact roles and responsibilities in cyber space may sometimes remain unclear. More generally, much attention has instead been focused on acquiring specific technical capacities and expertise to act in cyber space as decision-making procedures, doctrines for deployment and procedures may not always be clearly defined. For such reasons, there is a need to improve strategic decision-making as well as the ability to react to cyber crises.

In most cases, civilian ministries are responsible for co-ordinating incident response and the military is used only as an instrument of last resort. Moreover, in many countries, the military has little or no role in the protection of critical infrastructure. However, it has the responsibility for national defence, which presumably includes defence of the most extreme threats to critical infrastructure. The international community recognises this importance of protecting critical infrastructure. It is described as the backbone of our economies, security and health, and the Internet has become fundamental for the functioning of critical sectors that include energy, telecommunications, transport, health care and banking.[4]

One of the difficulties that might then arise is that where procedures might be outlined in formal doctrines and strategies, such procedures might not always be tested sufficiently in practice. Key players and organisations might still be uncertain about their exact responsibility. Good crisis management and incident response mechanisms should therefore clarify under what circumstances and through which procedures a request can be made for military assistance. In addition, testing these procedures and organisational capacity through realistic exercises should allow for better co-operation in a real crisis situation, and a whole-of-government approach is often recommended.

Public-Private Sector Relations: Enhancing Information Sharing And Trust

The significant role that the private sector has in this field has been particularly challenging for the military and security community. In some cases, a game-changing development has forced the way in which governments (military and intelligence) need to collaborate with the private sector. For instance, (1) militaries are increasingly dependent on civilian critical infrastructure which is becoming more network-enabled; (2) there is greater reliance on commercial products, with exposure to the same vulnerabilities faced by civilians and the private sector; and (3) critical military functions are becoming increasingly cyber-enabled.[5]

The sharing of actionable information on cyber threats and incidents remains a challenge both within many national governments, as well as between the public and private sectors. For instance, while the military and intelligence services may often be unable or unwilling to share classified information, the private sector might also be reluctant to share directly. However, both the public and private sectors require such information for alerts and threat warnings. In addition, this is also an area where recommendations have been made to promote the international exchange of best practices and lessons learned in public-private co-operation.[6]

Trust is important for information sharing, and such trust is often based on personal relationships. Especially since military and civilian cultures can diverge significantly, stakeholders should then develop a system where they meet personally or liaise regularly in order to better understand each other's needs, in order to build a more nuanced understanding of the other's perspectives and responsibilities, and to create points of contact. For example, scheduling weekly calls or monthly meetings can assist in building such relationships and therefore allow stakeholders to be more informed of developments across the field.

From a trust-building perspective, training can be valuable in that it may be applied both cross-sector as well as internationally. For instance, the European Union (EU) Cyber Defence Policy Framework of November 2014 highlights under its section on the promotion of civil-military co-operation that joint activities in the field of training and exercises will enhance co-operation.[7] It further highlights that this could reduce costs across different policy areas. Given the need to manage limited financial resources, this can only be beneficial for countries to consider as an initiative.

Trust is important for information sharing, and such trust is often based on personal relationships. Especially since military and civilian cultures can diverge significantly, stakeholders should then develop a system where they meet personally or liaise regularly in order to better understand each other's needs, in order to build a more nuanced understanding of the other's perspectives and responsibilities, and to create points of contact.

Managing Limited Financial And Labour Resoures

A regular complaint is that not only is there a shortage of cyber security experts, but both the public and private sectors are competing for available talent. More specifically, the recruitment and retention of skilled individuals in the armed forces itself is a challenge common to most jurisdictions. And while this is also the case for the civilian public sector and private sectors, the armed forces faces a particular challenge in attracting and retaining experts given the more profitable civilian domains. Furthermore, while it might be in the military's interests that the best talent be recruited, it also serves the national interest that such individuals are in the industry to support the economy. In addition, while there is a clear shortage of technical expertise, individuals who can translate the implications of technology to strategic choices and policy implications are also relatively scarce.

In order to alleviate this shortage, solutions that have been made include interdisciplinary education, and joint training of military and civilians so as to

enhance mutual understanding and create networks of trust. Moreover, in many countries, it is the private sector that supports the military with capacity, products and expertise—therefore the exchange of best practices in recruitment, training and retention, both between the public and private sectors and between international partners, might alleviate these shortages of experts to some extent.

Another issue that states must consider is the management of financial resources and the reduction of costs. Thus, by including industry and academia in exercises, this might mean both the harnessing of a pool of expertise and increased cost efficiencies.[8]

Leveraging Synergies With Other Civilian Actors

For similar reasons, leveraging the capabilities of law enforcement authorities might also mean the harnessing of expertise, and enhanced cost efficiencies. For example, the EU Cyber Defence Policy Framework recommends leveraging existing cyber crime prevention, investigation, and forensic capabilities in the development of cyber defence capabilities.[9] Furthermore, recommendations have been made to leverage law enforcement authorities' expertise by working with armed forces in post-conflict crises or natural disaster situations, where law enforcement might traditionally play a significant role in peacekeeping, capacity building, and reconstruction efforts. Such co-operation could be enhanced to increase cyber capacity building, and the expertise of regional and international law enforcement bodies that assist in building cyber capacity and capabilities might also be leveraged. This is especially noteworthy for the Asia-Pacific region, which is particularly prone to natural disasters.

INTERNATIONAL MILITARY CO-OPERATION, EXCHANGE AND DIALOGUE

This section focuses on military co-operation and dialogue. It analyses how to ensure that there are mechanisms to prevent further escalation when militaries are involved in managing these threats. In

Soldiers from the United States Marine Corps assisting in disaster relief efforts in the aftermath of Typhoon Haiyan in the Philippines in 2013.

other words, it highlights the importance of ensuring that actions are taken to prevent a possible escalation or conflict that may be sparked by a cyber-related incident. While the military might aim to be prepared to win in conflict, it should also be obliged to avoid escalation.[10] This section thus seeks to elaborate on mechanisms to avoid such escalation, even where the subject is considered sensitive.

If sufficient effort is made to ensure the right mechanisms are implemented to avoid misperceptions and misunderstandings, this article posits that cyber conflict is not inevitable—in the same manner that traditional conflict is not inevitable.

The unique aspects of cyber-related incidents have the potential to cause an escalation to armed conflict. One of the main concerns is the increasing potential for malicious cyber activities by state and non-state actors to create instability and mistrust in international relations. It is therefore important that the military ensures that there is international military-to-military dialogue, exchanges, and co-operation to alleviate possible tensions and prevent the escalation of conflict, especially in an environment where misperceptions could arise. Better forums for dialogue, exchanges and co-operation are needed so that there are mechanisms to prevent further escalation when militaries are involved in managing these threats. If sufficient effort is made to ensure the right mechanisms are implemented to avoid misperceptions and misunderstandings, this article posits that cyber conflict is not inevitable—in the same manner that traditional conflict is not inevitable.

International military-to-military co-operation for cyber-related matters is at a relatively early stage of maturity however, and countries are at different phases of development in this area. Moreover, a fixed structure for international military co-operation is lacking in outside organisations, unlike those within the North Atlantic Treaty Organisation (NATO), and the EU States will also continue to seek to develop or obtain capabilities. Consequently, there is an increasing concern over the lack of military-to-military dialogue in order to prevent miscalculations, misunderstandings, false attribution, or escalation in tensions. This is especially concerning regions, like the Asia-Pacific, where strong interstate tensions exist.

The international community recognises the need for international co-operation to reduce risks, and discussions are focused on reaffirming the applicability of international law to state behaviour in cyber space, as well as the development of voluntary, non-legally binding norms for responsible state behaviour in cyber space during peacetime. In addition, the need to develop and implement confidence building measures (CBMs) to increase stability and prevent the risk of conflict as a result of misperceptions and miscalculations arising from the malicious use of Information and Communications Technologies (ICTs) is recognised.[13]

Promoting More Multilateral And Bilateral Opportunities For Military Exchanges, Dialogue, and Co-operation

Improved international military dialogues, exchanges, and co-operation, whether at bilateral, sub-regional (this could be either inter-regional or intra-regional between like-minded countries), regional, or international levels could lead to better exchange of information to enhance cyber defence effectiveness and international stability.

Lessons learnt relating to processes as well as possible future challenges can be exchanged, and mutually-agreed action points might then be generated. Moreover, this does not need to be limited solely to militaries but can include other stakeholders to enhance international civil-military co-operation.

Such mutually-agreeable action points that could be generated through exchanges and dialogues to facilitate better co-operation are highly important. It is clear that while there is now, in the first instance, a level of agreement by high level officials on the need for states to co-operate as well as on possible areas where co-operation might be needed, currently there seems to be less clarity on specific mutually-agreeable action points and deliverables. Ideally, states should now begin to translate these agreements into real action points for implementation where none already exist.

The issue of trust then becomes significant again and it should not be underestimated in its role in facilitating better co-operation. Officers regularly cite it as key in creating these types of relations. The importance of creating an environment of trust, and enhanced transparency at national as well as international levels to foster an environment of stability needs to be emphasised. In addition, the role of personal relationships in building trust has been cited as very important if incidents arise, especially since problems can take years to resolve. Yet building trust may be easier to highlight and speak of as necessary than it is to achieve in real terms. For example, if there are serious tensions in state relations, it may be extremely difficult to surmount this challenge even when it is recognised as an essential component for enhanced co-operation on cyber-related matters.

Platforms such as the 2016 ASEAN-US Defence Ministers' Informal Meeting may help facilitate multilateral dialogue and co-operation to foster greater trust.

Soldiers from the Singapore Armed Forces (SAF) and Australian Defence Force (ADF) attending a joint briefing during Exercise Trident in Australia in 2014.

Increasing the levels of transparency is also regularly highlighted by government officers as key to ensuring an environment of stability as well as for developing common concepts in this domain. Such points are highly significant when there are recent concerns that are currently being echoed over an increasing environment of mistrust, especially in the Asia-Pacific region. Lastly, where possible, more effort should equally be made to ensure that there is better co-ordination and co-operation between initiatives across international and regional platforms. This should then create enhanced complementarity and avoid duplication of efforts.

A recent example from May 2015 of an initiative to increase co-operation in this area is that of the EU's Estonia-Latvia Presidency Cyber Hygiene Initiative proposed by two smaller EU Member States to increase awareness of and promote the need for basic cyber security standards within defence organisations covering human-related risk factors (this has apparently been a factor in more than 80 per cent of cyber incidents reported).[17]

Confidence Building Measures

Ideas derived from more traditional military-to-military CBMs like official military-to-military contact points and crisis communication procedures such as hotlines could assist in increasing such transparency, and reducing the risk of misperception in state behaviour and unwanted escalation. Stakeholders have suggested that existing common understanding, trust, and shared interests can also be built upon in order to enhance transparency and co-operation. Ultimately, this could then assist in strengthening existing structures or establishing structures where none exist in order to allow for stronger collaboration in future.

Where appropriate, there needs to be an increase in the level and regularity of military-to-military consultations and dialogue, information sharing on strategies, policies and institutional structures, joint exercises, as well as practical collaboration through bilateral or multilateral platforms. This further contributes to building mutual understanding and confidence. The exchange of information and best practices alone can help build trust as a starting point and prevent misunderstanding. For instance, while cyber security and cyber defence strategies may be quite different, their predominant role is the setting of goals and determining the means to achieve these goals, and such strategies have a strong declaratory function vis-a-vis other states. The right strategy can therefore present an opportunity to reduce the risk of conflict.

Small-step, military-to-military dialogues and other practical co-operation measures could additionally complement this objective of building confidence and improving international stability through international political agreement.

In terms of the current status of discussions over cyber, the exchange of national definitions or key terminology can further assist in building better understanding between parties and in alleviating the potential for misunderstandings between states. It has been suggested that an index or glossary of terms could even go some way to achieving this common understanding.

While pursuing international agreement on state behaviour in cyber space is desirable, there is still further space for possible progress by practical military-to-military dialogue or co-operation (as well as international civil-military co-operation) on cyber issues. Small-step, military-to-military dialogues and other practical co-operation measures could additionally complement this objective of building confidence and improving international stability through international political agreement.

States are therefore being encouraged to be more transparent about the roles and responsibilities of their defence forces and security services in the cyber domain as well as to pursue dialogue and other measures related to cyber issues to build confidence and ensure international stability.[19]

CONCLUSION

Although many of these points may not seem overtly new, they have not yet been fully resolved. This field is an evolving work in progress. In short, the principles of trust, transparency, and co-operation should be integrated within the majority of portfolios since there are few areas where cyber or ICT are not relevant. This is particularly important in order to mitigate the probabilities of escalation occurring on account of the nature of this field.

ENDNOTES

1. Heinl & Boeke, "Civil-Military Relations & International Military Cooperation in Cyberspace", University Leiden Campus the Hague, Research Project supported by The Netherlands Ministry of Defence, April 2015. Much of the material in this section is from this research project conducted in April 2015. The paper identified a non-exhaustive list of ongoing common global challenges and possible good practice solutions for a more effective response. In doing so, the paper reflected non-prescriptive inputs from a wide spectrum of global civil-military stakeholders including civilian agencies, the defence forces, academia and the private sector that emanated from an informal roundtable held in Singapore in November 2014.

2. Centre of Excellence for National Security Cybersecurity Workshop, "Cybersecurity: Emerging Issues, Trends, Technologies & Threats in 2015 and Beyond", Conference Report, Singapore, 20-21 July 2015.

3. This article does not outline the structure of decision-making at national level in Singapore. Rather it considers the more general challenges facing a majority of nation states in this field. In addition, in the past year a number of agencies have been established that house cyber expertise from across governments so as to coordinate the efforts of the civilian and military agencies.

4. Chair's Statement, *Global Conference on Cyberspace 2015*, n._20/21, 17 April 2015.

5. Centre of Excellence for National Security Cybersecurity Workshop, "Cybersecurity: Emerging Issues, Trends, Technologies & Threats in 2015 and Beyond", Conference Report, Singapore, 20-21 July 2015.

6. Chair's Statement, *Global Conference on Cyberspace 2015*, n._20, 17 April 2015.

7. Council of the European Union, *EU Cyber Defence Policy Framework*, 15585/14, 18 November 2014, 8.

8. Author's observations, Civil-Military Relations Panel, *Global Conference on Cyberspace 2015*, 17 April 2015.

9. Council of the European Union, *EU Cyber Defence Policy Framework*, 15585/14, 18 November 2014, 8.

10. Author's observations, Civil-Military Relations Panel, *Global Conference on Cyberspace 2015*, 17 April 2015.

11. Chair's Statement, *Global Conference on Cyberspace* 2015, n._29, 17 April 2015.

12. Chair's Statement, *Global Conference on Cyberspace 2015*, n._30, 17 April 2015.

13. Ibid.

14. Author's observations, Civil-Military Relations Panel, *Global Conference on Cyberspace* 2015, 17 April 2015.

15. Author's observations, *ASEAN Regional Forum Workshop on Cyber Security Capacity Building*, Hosted by the People's Republic of China and Malaysia, Beijing, 29-30 July 2015.

16. Ibid.

17. Centre of Excellence for National Security Cybersecurity Workshop, "Cybersecurity: Emerging Issues, Trends, Technologies & Threats in 2015 and Beyond", Conference Report, Singapore, 20-21 July 2015.

18. Author's observations, Civil-Military Relations Panel, *Global Conference on Cyberspace 2015*, 17 April 2015.

19. Chair's Statement, *Global Conference on Cyberspace 2015*, n._38, 17 April 2015.

20. Author's observations, Civil-Military Relations Panel, *Global Conference on Cyberspace 2015*, 17 April 2015.

Caitríona Heinl Caitríona Heinl joined the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies as a Research Fellow responsible for cyber analysis in October 2012. She has published peer-reviewed articles as well as both public and government policy advisory reports on topics that include engagement on emerging cyber challenges, international security and international cyber policy research, national security implications of emerging technologies. She currently holds a non-resident international fellowship with the Australian Strategic Policy Institute International Cyber Policy Centre, Canberra.

Ms Heinl previously led the Justice and Home Affairs policy group and Justice Steering Committee at the Institute of International and European Affairs (IIEA), Ireland. She qualified as a Solicitor in the UK (non-practising) and has been admitted as an Attorney-at-Law in New York. She is currently a member of the Irish government's Department of Foreign Affairs and Trade Foreign Policy Network.

Ms Heinl holds a Masters of Philosophy in International Relations from the University of Cambridge, having graduated in both commerce and law at University College Dublin and the Leopold Franzens University of Innsbruck in Austria with 1st Class Honours.