Cyber Warfare – from Science Fiction to Reality

Mika Kerttunen

Abstract: Cyber military capabilities promise better tactical and operational effects and better ways to conduct military operations. Despite the hype around cyber military development, the vast majority of armed forces are still focussing on preliminary capabilities such as situational awareness, information security and the protection of military networks. Yet, casual employment of available national cyber capabilities comes with a risk of escalation and creates a separate zone of dangerous legal opacity where e.g. human rights may be easily breached. States need to recognize the value of rule of law, stop de-valuing international legal order with opportunistic propositions and destabilizing practises, and agree upon responsible State practices in cyberspace.

Keywords: Cyber military operations, international law, international peace and security
Stichwörter: Cyber-Militäroperationen, Völkerrecht, internationaler Frieden und Sicherheit

1. Introduction

The list of cyber incidents is long: hardly a day goes by without news of revelations, data breaches, denial of service attacks and unexpected power outages. Social and new media have become a jungle of intensive commercial and aggressive political targeting and disgraceful social bullying. These millions of acts and attacks, and the dangers and vulnerabilities of our interconnected systems, do not, however, equal or constitute war. The fact that States are increasingly interested in developing military cyber capabilities does not mean that they are employing them irrespective of political, economic and military contexts and conflicts.

In contrast to the list of cyber incidents, the list of cyber military operations is surprisingly short. The Israeli operation Orchard provides an example of layered use of various means, including cyber assets to support otherwise rather blunt kinetic destruction of an alleged Syrian nuclear construction site in autumn 2007; and in the 2008 Russo-Georgian war the Russians synchronized their rather modest cyber operations with manoeuvre operations. On the other hand, Libicki in his analysis of the conflict in Ukraine goes to conclude that "the most notable thing about the war in Ukraine, however, is the near-complete absence of any perceptible cyber war" and that "the easy assumption that cyber attacks would unquestionably be used in modern warfare has come up wanting".[1]

The allegedly US-Israeli operation Olympic Games/Stuxnet (2010) malware is one of the most advanced undertakings, but it still can be better labelled as State power projection and a covert intelligence operation rather than as a military one. It nevertheless highlights a troubling tendency of blurring the line between civilian-run cyber-intelligence operations and military-run effect-causing cyberspace operations. The problems arising include the principal issue of the investigator, judge, and executioner becoming the same entity, and the covert, non-parliamentary nature of such politically motivated projections of State executive power.

The absence of clear examples and evidence of cyber military operations can be explained by three alternative scenarios: 1. States are not willing to use and reveal their true capabilities in secondary conflicts, 2. there have not been valuable and suitable targets that would have created the desired operational or political effects, or 3. that countries have the ability to penetrate most likely any system or network, but they have not yet fully harnessed that competence in systematic, doctrinal manner. Whatever the case may be, we have yet to witness the era of cyber warfare.

The article opens by situating the development of cyber military capabilities in a politico-strategic framework. This helps to understand the underlying rationality in developing and employing cyber military capabilities. After this conceptual framing, the article takes a doctrinal and military-operational view on cyber military operations. The analysis rounds up by discussing the implications of the political and military-operational proliferation of cyber military capabilities on international peace and security, including for the threshold to resort to use force in international relations and the established legal restrictions on hostile projection of State power. Ultimately, the analysis asks whether the development, deployment and employment of cyber means and methods – capabilities and techniques – change the *Clausewitzian* paradigm of war: war by its enduring nature being and remaining hostile, rational, and a play of chance.

The article warns that inflating the notions of war and weapons when referring of Information and Communication Technology (ICT) and overemphasising the needs of national security and extraordinary powers and measures create a vacuum between national and international jurisdictions, which leads to an erosion of legal order. It urges to find a shared understanding of responsible State behaviour in cyberspace and of how the employment of cyber capabilities can constitute an armed attack.

2. The political-strategic context

In their influential 1992 article Arquilla and Ronfeldt saw cyber war coming. They wondered whether it could help to avoid attritional conflict, be won by "striking at the strategic heart of an opponent's cyber structures, the systems of knowledge, information, and communications"; allow victory to be achieved without the need to maximize the destruction of the enemy.[2] Two decades later in an influential article of his, Rid, on the other hand did not see cyber war taking place.[3]

1 Martin Libicki, "Cyber War that Wasn't" in Geers, Kenneth (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO CCD COE Publications, 2015), pp. 49-54.

2 John Arquilla and David Ronfeldt, "Cyberwar is Coming!", *Comparative Strategy*, Vol. 12, No. 2 (Spring 1993), pp. 141-165.

3 Thomas Rid, "Cyber War Will Not Take Place",*Journal of Strategic Studies*, Vol. 35, No. 1 (February 2012), pp. 5-32.

DOI: 10.5771/0175-274X-2018-1-27

An oft-cited UNIDIR 2013 report provides an interim analysis of the state of development of military cyber capabilities. It counts 114 countries with national "cybersecurity programmes" and explains that these national agendas can range anywhere between basic network security and declared offensive cyber capabilities. The report lists 47 countries that give 'some role' in national cyber security to armed forces, a number frequently presumed as countries with military cyber capabilities. The report counts 27 countries having established or planned to establish specific military 'cyberwarfare' entities, 17 of which also comprise offensive military capabilities.[4] As with any novel capability area, the development of capabilities, in particular doctrines and skillful manpower, has been rather slow and modest.

Since 2012, the U.S. has been systematically reviewing its national strategies, joint military doctrines and field manuals to incorporate cyber capabilities as an elementary part of all military operations and functions. This would include deploying cyber units and teams also to tactical land forces formations, perhaps "down" to manoeuvre brigades, integrating cyber capabilities to the full range of military operations.

This qualitative and quantitative difference in the employment of information and communication technologies and cyber capabilities has widened the performance gap between developed and developing countries as well as among Western allies. Apart from the United States, very few countries have operational doctrines, cyber-specific units and established training and exercise regimes. Globally, the main trend is to create basic understanding, competence and capacity to protect military networks, systems and information. The desire to acquire both defensive and offensive cyber capabilities is yet growing.

Similar to proliferation of nuclear and other strategic weapons, the emerging spread of cyber military capabilities can be explained from instrumental, institutional, and identity perspectives:[5]

The instrumental claim refers to the actual military effects cyber capabilities are able to deliver. They are generally regarded as force multipliers increasing effectiveness in the battlefield.[6] Cyber operations as relatively cheap, yet far- and wide-reaching, and can thus be viewed as asymmetrical means that enable lesser countries to balance Western military technological supremacy and politico-strategic dominance.[7] The issue is of justice as well as insecurity. Many developing countries are wary of the free flow of information on Western terms as well as internally or externally triggered regime changes.

The institutional claim notices cyber capability development as part of military modernization and military cyber capacity also serving respective organizational interest and relative gains. For authoritarian regimes cyber tools are also handy tools of domestic control.

The identity claim emphasises the need of nations to modernize, but also in more concrete terms to be able to provide their allies, partners, and international investors interconnectivity, information, and ensured interoperability. Civilian and military cyber postures are evaluated, ranked, and verified by international donor and expert communities.[8] Those not meeting the standards are encouraged in the name of *capacity-building* to "improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfill their responsibilities; and bridge the divide in the security of ICTs and their use".[9]

Since 1998, the Russian Federation has invited the international community to identify and address threats to international peace and security resulting from development and use of information and communication technologies. The basic proposition of the process has been the threat of information war, and weapons as well as information as such, the latter being a possible avenue of malicious influence. The venue of Moscow's choice is the United Nations First Committee, also known as the Disarmament and International Security Committee.

Moreover, in the letter initiating disarmament talks on ICTs at the First Committee, Foreign Minister Ivanov moved information technologies and means of telecommunication from the more general discussions of the role of science and technology to the context of international security and disarmament (UN Resolution 43/77/A). Russia urged attention to the potential use of ICTs "for purposes incompatible with the objectives of maintaining international stability and security, the observance of the principles of non-use of force, non-interference in internal affairs and respect for human rights and freedoms". The focal points were the creation of 'information weapons' and the threat of information wars, which Moscow defined as "actions taken by one country to damage the information resources and systems of another country while at the same time protecting its own infrastructure".[10]

Russian concerns were directly linked to the development and demonstrated performance of U.S. information warfare concepts and capabilities. American information warfare doctrines of the mid-1990s, written in the euphoric fallout of the – militarily speaking – highly successful 1991 Gulf War against Iraq, leaned on overwhelming information superiority and, echoing Arquilla and Ronfeldt, promised affecting adversary information, information-based processes, information systems, and computer-based networks. The U.S. doctrine also widened

4 United Nations Institute for Disarmament Research, *The Cyber Index International Security Trends and Realities* (2013), pp. 1-3. The report does not elaborate these concepts and its criteria.

5 On arms race and nuclear proliferation see e.g. Raimo Väyrynen, *Ydinaseet ja suurvaltapolitiikka* (Helsinki: Tammi, 1982); Scott D. Sagan, "Why Do States Build Nuclear Weapons. Three Models in Search of a Bomb", *International Security* Vol. 21, No. 3 (1996), pp. 54-86.

6 The Netherlands Ministry of Defence, *The Defence Cyber Strategy* (27 June 2012), p. 11.

7 See Adam P. Liff "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", *Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012), pp. 401-428.

8 See e.g. The World Economic Forum, *The Global Information Technology Report 2015. ICTs for Inclusive Growth*; the International Telecommunication Union, *Global Cybersecurity Index & Cyberwellness Profiles* (April 2015); Global Cyber Security Capacity Centre, *Cyber Security Capability Maturity Model (CMM)*, Oxford University (15 December 2014); and, International Cyber Policy Centre, *Cyber Maturity in the Asia-Pacific Region*, Australian Strategic Policy Institute (2015).

9 United Nations General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174 (22 July 2015).

10 United Nations General Assembly, "Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General", A-C.1-53-3, (30 September 1998).

the use of information warfare means and methods beyond "a military conflict, declared or otherwise".[11]

Russian concerns are shared by China and many developing countries. Setting the politico-strategic motivations of technologically inferior and domestically insecure nations to curb a potential adversary known to take the role of a global constable, *Captain America*, four claims are relevant for the purposes of this study that the development, deployment, and employment of ICT capabilities will:

- Lower the threshold to project State power;
- Increase the numbers of State-to-State conflicts;
- Escalate internal and State-to-State conflicts;
- Provide criminals and terrorists with destructive cyber capabilities.[12]

The Western normative approach to address the problems States, businesses, and individuals are exposed to is not to limit the development and deployment of ICTs. Rather, it is to strengthen adherence to international law, in particular the UN Charter, human rights and international humanitarian law, to develop norms, rules and principles of responsible State behaviour, and to develop confidence-building measures for cyberspace.

On the other hand, it is similarly logical to consider that increased interdependency of global systems and services, and the unclear legitimacy of cyber operations can urge caution; and that less destructive cyber operations may decrease the overall destructiveness of conflicts.[13] It should also be mentioned that Russia and China, too, are developing national and military tools of information contestation and warfare.

3. Cyber operations and warfare

Cyber (or cyberspace) operations are employed to create better results (effects) or to create anticipated effects in better ways.[14] What constitutes 'better' in terms of military operations is subject to deontological and consequential assessments.

Military commanders, armed forces as well as their political, civilian masters emphasize the operational values of speed, stealth, and precision, but also economy of action and effect the use of cyber capabilities can provide. Occasionally, more devastating and long-lasting destruction is considered necessary; sometimes a limited one is deemed sufficient. Regarding the use of conventional, so called kinetic capabilities, military theory and manuals used to provide enough rough guidance and calculations. In terms of cyber effects such scientific approach to war would be even more impotent. The fallacy of such rationality is that although first-order effects can be estimated, the second- and third order outcomes, for example on spill-over effects, societal stamina, and political will, are next to impossible to calculate.

The employment of advanced information and communication technologies in violent military activities can be understood in a continuum of no-ICTs to ICT-supported-and-assisted to only-cyber activities. Table 1 illustrates this horizontal division. It also situates the employment of ICT/cyber capabilities vertically according to the levels of military activities: engagement (battle), operation, campaign, and war.

Table 1. The use of ICT and cyber means at various levels of violent military activities.

	No ICTs used	**ICTs supporting and assisting (in)**	**Only cyber means used (in)**
War	Not likely	Joint functions	Not likely
Campaign	Unlikely	Joint functions	Unlikely
Operation	Brute violence	Joint functions	Computer network operations, Information operations
Engagement	Brute violence	Joint Functions	Computer network operations, Electronic warfare, Signal intelligence, Information operations

Source: Author's compilation.

Such vertical typology of war, points out that although engagements, operations or series of concerted battles, and campaigns or series of synchronized operations all are characteristics of war, war as a social-political phenomenon is more than a product of its local constituencies; it is an inseparable system of whole of which emerges from and amplifies its initial conditions.[15] In practical terms, the employment of cyber capabilities does not create wider, long-term and decisive effects that military campaigns and war proper aim to achieve. The question is not one of the possibility of death and destruction legal rulings of war are looking for, but the scope of (such) violent, devastating and painful effects.[16] Moreover, as technical, tactical and operational cyber effects start to accumulate, the infected side becomes prone to turn to kinetic weapons and

11 Joint Chiefs of Staff, *Joint Doctrine for Command and Control Warfare* (JP 3-13.1), (7 February 1996), pp. I-3; Department of Defense, *Information Operations,* Directive No. S-3600.1 (9 December 1996).

12 See for example the United Nations General Assembly, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", A/70/174 (22 July 2015); and VII BRICS Summit, *Ufa Declaration* (9 July 2015).

13 When accepting the common understanding of the STUXNET – Saudi Aramco/U.S. banks attacks as exchanges between the U.S./Israel and Iran, the low level of destructive State power should be noted. The kinetic alternative of bombing the Natanz nuclear enrichment plant would have led to greater destruction and most likely stronger retaliatory measures. In this light, the Stuxnet episode was not very successful by outcome, but revealed countries' surprisingly permissive, or helpless, attitude towards the employment of even offensive cyber capabilities.

14 Computers have been used for military operational purposes since 1940s to calculate trajectories and favourable attack patters, since 1950s to ensure safer and faster communications, since 1960s to analyse vast amounts of intelligence data, and since 1970s to improve accuracy of intelligence and targeting. Since 1990s computing, radiophony and telephony have merged to current smart and interconnected technologies.

15 Other typologies of war for example account its domains as arenas of warfare (land, air, sea, space and cyber) or specific tactics or technics employed in waging it (guerrilla, mine, submarine warfare). Another vertical typology of war includes the levels of war of strategic, operational, and tactical.

16 For the death-and-destruction doctrine see e.g. Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *The Columbia Journal of Transnational Law*, Vol. 37 (1999), pp. 885-937; Michael N. Schmitt, "Cyber Operations and the *Jus in Bello*: Key Issues", *International Law and the Changing Character of War, International Law Studies* No 87 (2011), pp. 89-110; Thomas G. Mahnken, "Cyber War and Cyber Warfare," in Kristin M. Lord and Travis Sharp (eds.), *America's Cyber Future: Security and Prosperity in the Information Age* (Washington, D.C.: Center for a New American Security, 2011); Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1 (February 2012), pp. 5-32; Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, Vol. 192 (March/April 2012), pp. 80-84.

war. Here political decision-makers face a line drawn in water: whereas cautious use of cyber means risks remaining ineffective, their effective use risks igniting conflict. Conceptually, the notion of *cyber war* turns means to an end and assumes that cyber means are and can be employed isolated from political tensions and socio-strategic tendencies. A conceptually correct and factually accurate notion to explain and entertain the development, deployment and employment of ICTs and cyber military capabilities is *cyber warfare*, a combination of ways and means, methods and capabilities, tools and their use.

It is relatively straightforward to account for how ICTs are used to support and assist the core military functions of command and control, intelligence, fires, manoeuvre and movement, protection, and sustainment in the full scale and scope of military activities.[17] The following table exemplifies the use of ICTs in joint functions.

Table 2. The use of ICTs in military joint functions

Joint Function	**Role, purpose or function of activities**	**Examples of systems and solutions**
Command and Control	Assistance to planning and decision-making, monitoring and reporting Situational awareness Secure communications	Modeling Artificial intelligence Smart displays and overlays Deployable, mobile and secure networks
Intelligence	Gathering, analyzing and disseminating intelligence information Situational awareness Early warning	Penetration tools Spyware Computerized analyses of 'big data' Weak signals analysis War-gaming (red team)
Fires	Targeting Positioning Deception Interference Denial Destruction Influence	Global Positioning Systems Precision weapons Electronic warfare Computer-network attacks: denial of service; destruction of networks, nodes or information; dissemination of disinformation
Movement and Maneuver	Positioning and navigation Situational awareness Deception Movement control	Smart maps Digital overlays
Protection	Network protection Information assurance Resiliency and recovery Camouflage Denial of the spectrum	Layered defence Keys, algorithms and cryptology Computer Emergency Response Teams Malware detection Malware-sharing platforms Electronic deception and camouflage Jamming
Sustainment	Situational awareness Assistance to planning, monitoring and reporting	Modeling Asset tracking Battle damage assessment Real-time medical monitoring and reporting

Source: Eneken Tikk-Ringas (ed.), Evolution of Cyber Domain (London: Routledge/IISS, 2016), p. 163, referring to tested or already applied practices among technologically advanced, predominately Western armed forces.

Another question is what constitutes cyber operations and capabilities. In general, a capability is perceived as the capacity to perform an action, or the elements that facilitate such a capacity. The former view – which covers, inter alia, situational awareness, network protection, force projection, and resilience as well as recovery – mixes qualities and activities; the latter, in its narrowest interpretation, focuses on materiel, especially devices and programs. A wider perspective typical in national or organizational capability development also covers intangible elements such as doctrine, concepts, training, and availability, as well as deployability.

National approaches to cyber operations differ. There are three rather distinct categories in Western military doctrines: computer-network or cyberspace operations, electronic warfare, and information operations. The main differences between countries arise in the relation between information operations and cyberspace/computer-network operations as either hierarchical, parallel or separate activities. The U.S. doctrines have come to separate *cyberspace operations* seeking to create effects in and through cyberspace from *information operations* that seek to create cognitive-psychological effects.[18] Computer network operations constitute the core and main method of cyber attacks, operations and warfare.[19] A narrow interpretation of cyber operations would then refer to electronic and electromagnetic means and methods to create designated effects on adversary information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[20] The designated effects can vary from manipulation, tampering of data (information) to denials of access to data, systems and networks to partial or complete disruption, degrading or destruction of data, devices and networks.[21]

17 Also known in U.S. military culture as *joint functions*. This limitation thus leaves in particular non-violent administrative tasks, e.g. payroll and education and exercises, aside.

18 Joint Chiefs of Staff, *Cyberspace Operations* (JP 3-12 (R)) (5 February 2013), pp. I-5-I-6, II-1.

19 Adam P. Liff, in line with computer scientists, regards "cyberwarfare as a state of conflict between two or more political actors characterized by the deliberate hostile and cost-inducing use of CNA against an adversary's critical civilian or military infrastructure with coercive intent in order to extract political concessions, as a brute force measure against military or civilian networks in order to reduce the adversary's ability to defend itself or retaliate in kind or with conventional force, or against civilian and/or military targets in order to frame another actor for strategic purposes" (Adam P. Liff "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", *Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012), pp. 401-428).

20 Following the U.S. military definition of cyberspace:"a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (U.S. Joint Chiefs of Staff, JP 6-0 *Joint Communications*, 10 June 2015). See also The White House, PPD-20 *U.S. Cyber Operations Policy* (16 October 2012), and the International Telecommunication Union definition of ICTs comprising "a broad and unconsolidated domain of products, infrastructure and processes that include telecommunications and information technologies, from radios and telephone lines to satellites, computers and the Internet" (ITU, *Measuring Information Society Report 2015*).

21 PPD-20; USSTRATCOM, *The Cyber Warfare Lexicon. A Language to support the development, planning, and employment of cyber weapons and other modern warfare capabilities* (5 January 2009), pp. 4-12.

China and Russia do not discuss the idea of cyber operations but speak of information warfare, which covers the three main categories. China and Russia are not as advanced as the U.S. in integrating cyber capabilities into all military operations and functions but are known for their network operations ("hacking"), electronic warfare and signal intelligence competences.[22]Summarizing, a streamlined typology of cyber military operations would thus consists of:

- Computer Network Operations (CNO) including computer network attacks to disrupt, deny, degrade or destroy information resident in a computer or computer network, or destroy or damage the computer or computer network itself; computer network defense to protect data, information, networks, net-centric capabilities;[23]
- Computer Network Exploitation (CNE) to acquire information about computers and computer networks, by gaining access to information hosted on those and the ability to make use of the information and the computers/computer networks;[24]
- Electronic Warfare (EW) (operations) exploiting the electromagnetic spectrum to create effects on the enemy networks and systems by mainly the use of electromagnetic energy, directed energy, or anti-radiation weapons to degrade, neutralize, or destroy enemy combat capabilities and to protect own systems and services from any harmful effects of friendly or enemy use of the electromagnetic spectrum;[25] and
- Signal Intelligence (SIGINT) as a specific technique and branch of intercepting, collecting and analyzing electronic signals (communication and non-communication emitters) to create intelligence information. It is subdivided into three subcategories of communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence.[26]

A broader reading could also encompass:

- The use of ICTs in military operations and functions of command and control, intelligence, fires, manoeuvre and movement, protection, and sustainment; and
- Information Operations (IO, Info-ops) encompassing elements such as strategic communication, public affairs, civil-military operations, cyberspace operations, information assurance, space operations, military information support operations, intelligence, military deception, operations security, special technical operations, joint electromagnetic spectrum operations, and key leader engagement.[27]

For advanced capabilities needed in computer network operations, the 2012 DARPA *Broad Agency Announcement* on "Foundational Cyberwarfare (Plan X)" offers deeper insights on a conceptual cyber battlespace. The purpose of the Plan X is to build an end-to-end system that enables "military to understand, plan, and manage cyber warfare in real-time, large-scale, and dynamic network environments.[28] The system DARPA envisions would contain improved abilities of e.g. situational awareness, offensive penetration and fires as well as movement, manoeuvre and sustainment within cyberspace.[29]

Computer network operations can be conducted at national level for politico-strategic purposes, at regional or theatre level for operational purposes and at local, tactical level for often immediate purposes and objectives. In addition to conduct ongoing operations, malware and spyware, or more general code, can be prepositioned in adversary systems to be activated when needed. Such versatile use and utility make cyber capabilities a lucrative option to be deployed.

4. Considerations for international peace and security

So what? The vast majority of all questionable electro-magnetic signals, attacks, exploits and incidents in cyberspace are conducted by civilian security and intelligence agencies, as well as criminals, terrorists and individual hackers – and not by armed forces.[30] However, some countries deliberately task or buy hacking or espionage services from criminal groups. Also true is that in some countries national intelligence and security services are militarily organized, and that the armed forces align with authoritarian rulers and regimes.

Therefore, the most effective solutions to improve national cyber security – *inter alia* the protection of networks and infrastructure and improve information security and privacy – are civilian, political and educational rather than military or international. Instead of *war*, a more accurate and appropriate framing for the massive cyber problems would be individual incompetence, lack of national responsibility and due diligence, and international insecurity and injustice. It is admittedly convenient for

22 Mark Stokes, Jenny Lin and L.C. Russell Hsiao, 'The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Structure', *Project 2049* (11 November 2011), pp. 4-13. See also Timothy L. Thomas, *Three Faces of the Cyber Dragon: Cyber Peace Activist, Spook, Hacker* (Fort Leavenworth, KS: Foreign Military Studies Office, 2012), pp. 97-100; Larry M. Wortzel, 'The Chinese People's Liberation Army and Information Warfare', (Strategic Studies Institute (March 2014); and Amy Chang, *Warring State. China's Cybersecurity Strategy*, Center for New American Security (December 2014). Cf. James P. Farwell and Darby J. Arakelian, "Using Information in Contemporary War", *Parameters* Vol. 43, No. 3 (Autumn 2016), pp. 71-86, who state that information warfare is of changing behaviour, and list information warfare tactics to include information dominance, humour, operational shock, reflective control and weaponized social media.

23 JP 3-12 (R), p. II-2-II-3; NATO, *Allied Joint Doctrine for Information operations* (AJP 3-10) (November 2009), pp. 1-7.

24 AJP 3-10, pp. 1-11.

25 Joint Chiefs of Staff, *Electronic Warfare*, (JP 3-13.1) (25 November 2007), pp. I-2-I-4; Headquarters, Department of the Army, *Cyber Electromagnetic Activities*, Field Manual No. 3-38 (12 February 2014), p. 4-1-4-4.

26 Joint Chiefs of Staff, *Joint Intelligence* (JP 2-0) (22 October 2013), p. B-5-B-6.

27 Joint Chiefs of Staff, *Information Operations* (JP 3-13) (20 November 2014), p. II-5-II-13. Note that the concept of information operations is an integrating function that employs several capabilities, but do necessarily command (possess) them. It utilizes for example staff elements, communication systems and organizations as well as cyber capabilities to plan, deliver and assess its operations and effects.

28 Defence Advanced Research Projects Agency, *Broad Agency Announcement*, "Foundational Cyberwarfare (Plan X)", DARPA-BAA-13-02 (20 November 2012) pp. 8-9.

29 Ibid, pp. 6-8. See also Andrew Blyth, "Computer Network Operations (CNO)" in Bidgoli, Hossein (ed.) *Handbook of Information Security*, Vol. 2: Information Warfare; Social, Legal, and International Issues; and Security Foundations (Hoboken N.J.: John Wiley & Sons, 2006), pp. 89-100; and Simon Hansman and Ray Hunt, "A taxonomy of network and computer attacks", *Computers and Security* (2004).

30 Statistic accounts and best estimates claim that as of February 2017 of all cyber attacks (signals) 64.5% are cyber crime, 22.4 % espionage, 7.9% hactivism and 5.3% of what can be classified as cyber warfare (hackmageddon.org). The website, which does not explain its criteria, state that in 2016 cyber crime had raised from 67% to 72.1%, hacktivism dropped to 14.2% from 20.8%, cyber espionage had been stable (9.8% v. 9.2%), and cyber warfare had nearly doubled its share (4.3% vs 2.4%).

governments, tempting for the private sector and easy for interest groups to be concerned of military operations, but here the military sector is more a usual suspect than the real culprit.

Yet, cyber military capabilities are developed. An exercise of combining the frequency of cyber military employment (*more* or *less*) and the quality of effects (*better* or *worse*) will provide us with four potential paths of development:

- Better and/but more: Cyberspace operations manage to create desired, precise effects without death and destruction or spill-over and escalation. Despite the increased tendency of multi- or unilaterally to employ cyber capabilities to various local, regional or global conflicts, death, destruction and politico-socio escalation of such conflicts will reduce.
- Better and/but less: Despite of cyberspace operations managing to create desired and targeted effects without death and destruction or spill-over and escalation States deploy them only with caution and in accordance with internationally agreed norms and principles.
- Worse and/but less: Because cyberspace operations create uncontrollable effects in and outside of cyberspace, causing not only damage to data and ICT systems but also to industrial and societal systems and functions, States deploy them with caution and in accordance with internationally agreed rules, norms and principles.
- Worse and/but more: Despite of the uncontrollable effects in and outside of cyberspace, States consider cyber capabilities effective forms of power projection across various political, economic, military and social arenas and conflicts.

The genie is out of the bottle, and hostile coding and evil power projection cannot be wished away. Limiting the development of information and communication technologies that are predominately in the hands of private industry and utilized by billions of people would not succeed either. ICTs provide and promise individual, economic and societal rewards. International normative processes are slow or deadlocked. Emphasizing each "State's accountability for mitigating international cyber threats", as Tikk recommends, would offer a reset.[31]

States need to take responsibility of their cyberspace and action. Three moves would take national and global cyber security ahead. First, having a national cyber security strategy should become a norm, an expectation of responsible State behaviour and government accountability before the people and the international community. That some 70 countries have issued a strategy, several of them on their second or third turn, cannot hide the fact that close to 120 countries are without such explicit political and administrative guidance.[32] States declaring their intentions and overriding principles in cyber defence would increase transparency and remove doubts and unsubstantiated claims.

Secondly, States need to subscribe to the notion of due diligence in cyberspace. The International Law Commission's commentary on the "Prevention of Transboundary Harm from Hazardous Activities" explains well the *raison d'être* of due diligence and is worth a lengthy reference:

> "The obligation of the State of origin to take preventive or minimization measures is one of due diligence. It is the conduct of the State of origin that will determine whether the State has complied with its obligation under the present articles. The duty of due diligence involved, however, is not intended to guarantee that significant harm be totally prevented, if it is not possible to do so. In that eventuality, the State ... [must] exert its best possible efforts to minimize the risk. In this sense, it does not guarantee that the harm would not occur." [33]

Thirdly, a more determined take on confidence and security-building measures is needed. We should not be satisfied with the established approach from transparency and communication to sectorial and contingent cooperation to (possibly some) restraint mechanism-action. This marching order consumes much time and political energy. As potential adversaries do not like or trust each other, they are less enthusiastic to share and collaborate. Yet they need, and politically afford, to reduce the risk of conflicts and employ stability and restraint mechanisms – another slow-train-coming, but at least the right train.

5. Conclusions

Amidst all fears, insecurity and technological enthusiasm it is useful to reconsider and recognize five concluding suggestions:

- Being vulnerable and valuable is a prerequisite for potentially becoming targeted, but not a reason to go to war; [34] on the contrary, being mutually vulnerable can encourage caution, even cooperation;
- Possessing defensive, offensive and intelligence cyber capabilities does not make States randomly belligerent; on the contrary, States use them in the context of political disputes, confrontation or conflicts;
- Being attacked, exploited or bashed in cyberspace even by an adversary nation-state does not translate to war; the opposite however is true, in war and major campaigns, most likely also in international crisis response and peacekeeping operations, computer network attacks, electronic attacks and propagandist information operation will take place;
- Cyber capabilities offer seemingly easy ways to promote one's political and operational objectives in peacetime, disputes and conflicts; in the absence of a clear understanding of what constitutes responsible and acceptable State behaviour and how international law can be applied in cyberspace, such use comes with high risks of escalation, even unintentional escalation;
- The possibility to conduct effective activities in and through cyberspace does not replace physical violence or necessarily make war, death and destruction less reasonable options;

31 Eneken Tikk, "Cyber: Arms Control Without Arms?" in Koivula, Tommi and Simonen, Katariina, *Arms Control in Europe: Regimes, Trends and Threats* (Helsinki: University of Helsinki, 2017).

32 Mika Kerttunen, "National Cyber Security Strategies – A Normative Reading" in Tikk, Eneken (ed.) *Normative Considerations of International Cyber Security* (T.M.C. Asser Press, forthcoming 2018).

33 Report of the International Law Commission, 53rd Session, UN Doc. A/56/10 (2001), p. 154.

34 Cf. Kristan Stoddard, "Live Free or Die Hard: U.S. –U.K. Cybersecurity Policies", *Political Science Quarterly,* Vol. 131, No. 4 (2016-17), pp. 803-842.

neither have the tendencies of war, violence, chance and (im)probability and instrumentality, been changed.[35]

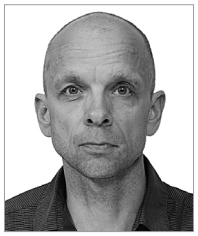
Cyber capabilities are expanding the range of possible harm and outcomes between, and in fact within, the concepts of war and peace.[36] States, sub-state and non-state actors exploit not only technical vulnerabilities, but most importantly lack of awareness, lack of responsibility and lack of consensus of what behaviour is tolerable and what is not.

'Signals', 'incidents' or 'attacks', regardless of their number, thousands or millions a day, week, month or year, do not constitute cyber- or any other war in a political, legal, operative or factual sense. War-framing is a linguistic-populist move that sells fear and supports the motley crew of governments, defence sector, cyber security industry, peace and disarmament activists and the prophets of anti-establishment in their focussed purposes. Similarly, mongering is aligning information technologies with weapons of mass destruction: the mere fact that millions of human beings can be made victims or unknowing culprits does not justify the terrifying injections of fear and the undermining of the real victims of nuclear radiation and poisonous gas clouds.

Irrespective of whether we are concerned of national, human or information security, privacy or world peace, cyber dangers are to be taken seriously. Regarding everything from petty hacking to economic espionage, from fraud to phishing, and from the use of ICTs for terrorist purposes to integration of cyber capabilities in military operations, a raging war does not help to identify, let alone solve issues of international peace and security. Most importantly, such framing prohibits us to acknowledge that information and communication technologies are first and foremost tools of peace and prosperity, empowerment and development.

The tendency of treating cyber issues that could be solved with basic safety, security and law enforcement measures, requiring military solutions and warring by nature shifts the problems and solutions outside of normalcy. It leads to calls for extraordinary measures, extrajudicial mandates and extraterritorial rights. The inflation of the exceptional inevitably lowers the threshold to resort to force and legitimizes interventions, interferences and breaches of human rights.[37] It separates the threshold of use of force from the threshold of armed attack, and creates a zone of dangerous opacity. If a cyber attack, operation or campaign does not constitute an armed attack, victim States and the international community have very few legitimate means to response, and most essentially self-defence as authorised by Article 51 of the United Nations Charter would be ruled out. On the other hand, if the determination of an armed attack is left to individual countries to decide, even minor cyber attacks can escalate into international and armed conflicts. The wedge between the thresholds allows the hybrid forces of anxious States and terrorist and criminals to roam undisturbed also, but especially in cyberspace. The inflated climate of war ultimately erodes international legal order and deflates the protection of civilians from the effects of conflict and war. The space between the two interpretations of armed attack needs to be filled with internationally agreed principles and norms of responsible State behaviour in cyberspace. In short, as unrealistic it may sound, States need to re-cognize the value of the rule of law, the democratic rule of law, and stop de-valuing international legal order with opportunistic under-the-belt propositions and destabilizing practises.

Although the time is not ripe for an international agreement on appropriate cyberspace behaviour, global cyber security or national cyber defence, the need and time for such broader consensus is likely to come. It will probably take years for serious incidents to happen and for increasing state practise, good and not so good, to emerge before we start to grasp what is to be done.



D.Soc.Sc. (Pol.), LTC (ret. FI A) **Mika Kerttunen** is Director of Studies, Cyber Policy Institute (Tartu, Estonia). He is a graduate of the Finnish Military Academy and General Staff Officer Course as well as the Royal Norwegian Command and Staff College. Kerttunen studied world politics at the University of Helsinki and analyzed in his 2009 dissertation Indian foreign and nuclear policy. After his military service he has been focusing on international cyber diplomacy, cyber norms development, and analyzed the development of national cyber security strategies and military cyber doctrines. Mika Kerttunen served as advisor to the Finnish expert at the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2016-2017). He is Visiting Faculty Member at the University of Tartu Law School and Senior Advisor to ICT for Peace Foundation.

35 Carl von Clauswitz, *Vom Kriege* [1832] (Köln: Ferd. Dümmler Verlag, 1991), Buch 1, Kapitel 1:28. It should be noted that Clausewitz's *wunderliche Dreifaltigkeit* is not a desired objective but his observation of war.

36 Lucas Kello, "The Meaning of the Cyber Revolution. Perils to Theory and Statecraft", *International Security,* Vol. 38, No. 2 (Fall 2013), pp. 7-40.

37 Krisch observes similar rise in new rights of intervention and to use force (Nico Krisch, "International Law in Times of Hegemony: Unequal Power and the Shaping of the International Legal Order", *European Journal of International Law*, 16 (2005), pp. 369-408); accordingly treating national and international terrorism an issue of national security instead of one of (national) law enforcement witnesses of the tendency to *securitize* certain problematic issues.