Cyberspace from the Hybrid Threat Perspective

Håkan Gunneriusson[1] and Rain Ottis[2, 3]
[1]Swedish National Defence College, Stockholm, Sweden
[2]University of Jyväskylä, Jyväskylä, Finland
[3]Tallinn University of Technology, Tallinn, Estonia
rain.ottis@jyu.fi

Abstract: Hybrid threats use conventional and unconventional means to achieve their goals. In this paper we explore the cyber threats as one possible aspect of hybrid threats. We describe three ways of approaching cyberspace (operations) from the hybrid threats perspective: supporting conventional operations, exploiting non-military systems, and exploring the opportunities provided by this environment. In particular, we highlight the aspects that are or likely will be relevant to the military community.

Keywords: hybrid threat, cyberspace, cyber operation, Internet, military

1. Introduction

One of the problems with the concept of hybrid threats is that it is very difficult to define. Hybrid threats are not defined by the actors, since states, non-state actors and even individuals might be considered (part of) hybrid threats. They are not about some specific technology, since the list here keeps growing as new technologies become available. They are not about specific effects, as a hybrid campaign may result in casualties, changed decisions, altered public perception, etc. Perhaps the best way to put it, hybrid threat is a manifestation of total war. It is about making the other side submit to one's will, with any means available.

Threats from or using cyberspace are similarly difficult to define, and can in fact be viewed as a subset of hybrid threats. Cyber threats come in the form of state actors, criminal groups, terrorist organizations, hacktivists, professional hackers for hire (mercenaries), etc. The list of exploitable technologies also keeps growing – aside from servers, personal computers and laptops we also have to worry about smart phones, smart meters (electricity distribution to our homes), wireless-enabled pacemakers, industrial control systems, etc, and that is just the hardware side. Possible effects can range from tongue-in-cheek publicity campaigns to destruction of critical infrastructure components and potentially – deaths.

Cyber threats operate in a man-made environment. As such, they are constrained by the capabilities built into that environment. However, this is in fact an enabler for the cyber attacker. Non-trivial man-made systems (such as computers, airplanes, etc.) are rarely perfectly implemented and may be based on flawed design assumptions. These assumptions may be about type of input, length of input, number of simultaneous user sessions, etc. Cyber attacks work by exploiting design assumptions or implementation flaws. It is important to realize, however, that while cyberspace is the “home” environment for cyber threats, they can and do affect other environments as well. Consider, for example, the case of StuxNet, where a cyber-attack disrupted the uranium enrichment process and caused a number of physical devices to break in Iran. (See, for example, Falliere, Murchu and Chien 2011, Sanger 2012, The Economist 2010a) Or consider the case of cyber-attacks against Georgian government and news sites during the 2008 Russia-Georgia war, which hampered the Georgian government's ability to communicate with the citizenry. (Markoff 2008)

These risks from cyberspace have a serious effect on society. On one hand, we are concerned with various threats – hacktivists, criminals, spies, etc. In order to protect ourselves (our systems, our data, our way of life) we are constantly endeavoring to improve the security situation in cyberspace. On the other hand, however, we are concerned with the opportunities and liberties associated with cyberspace – freedom of speech, privacy, etc. Unfortunately, in many cases, an increase in security tends to undermine the open and liberal society. Therefore, it is important that (military) security professionals are aware of these concerns and will take steps to minimize the adverse effects of new security solutions.

In this paper we describe three ways of approaching cyberspace (operations) from the hybrid threats perspective. In an effort to better explain this new type of threat to commanders, planners and soldiers, we highlight the aspects that are or likely will be relevant to the military community.

2. Hybrid threats in relation to cyber threats

Hybrid threat as a concept has changed over time. This is not unusual when it comes to the combination of the military culture and theoretical concepts. The now dead acronym EBO (Effects Based Operations) had a similar story. (See, for example, Mattis 2008 or Ho 2005) The stake holders agreed that the term held some truth but they could not come to an agreement of the content or meaning of the concept. The terms used in EBO were so hollow yet so widely discussed that it was considered better to leave that debate open and to concentrate on developing our theoretical thinking on military operations instead.

The initial meaning of hybrid threat was described as a non-state actor wielding a conventional capability as if it were a state-actor. (Matthews 2008) The concept has evolved to a catch-all phrase for unconventional and unexpected threats which strike asymmetrically. Now, as with EBO, NATO has abandoned the development of the concept of hybrid threats. However, this does not mean that the underlying concept is not of any use.

In the early days of the Internet, many wondered about the possibilities that global networking would bring. In historical terms, this was similar to the time when electricity was harnessed for the benefit of society. Such advances in science and technology bring about all-encompassing effects to the entire society, not just specific markets, businesses or governments. Instead of talking about, for example, *the electricity threat* or *the cyber threat,* it might be better to use the hybrid threat concept as a way to describe the interplay between conventional and unconventional threats to our society. In this paper we have taken this route in order to explore the cyber threat from a new perspective, since the military is already somewhat familiar with hybrid threats.

Although this is not a firm rule, hybrid threats tend to target the civil society rather than the military. This is a double asymmetry as it both strikes in unconventional ways and targets parts of society that may not be prepared for the attack. Defending against cyber threats requires a comprehensive approach, involving all relevant stakeholders from responsible government agencies (including the military) to private companies to individuals.

3. Cyberspace and cyber operations

Cyberspace is the extension of some of the greatest technological developments of the 20th Century: the electronic computer, the Internet and the World Wide Web. In 1948 Norbert Wiener coined the word cybernetics, which refers to “communication and control in the animal and the machine” (Wiener 1948). The discipline of cybernetics plays an important role in understanding and developing the underlying infrastructure of cyberspace. In 1984 William Gibson, a science fiction writer, first used the term cyberspace to describe the “consensual hallucination” of a new domain formed by interconnected computers. (Gibson 1984) Over the last decade the term has been widely adopted, but there are numerous ways of defining, interpreting and using the underlying concept.

One of the most prominent concepts of cyberspace is the one that has emerged in the national defense and security sector. It refers to cyberspace as a new domain of (military) operations, on equal footing with land, air, sea, and sometimes – space. (The Economist 2010b) The western military doctrine generally divides the operations in cyberspace into two or three categories. Perhaps the best known is the US approach, which uses the term ‘computer network’ instead of ‘cyberspace’. According to this doctrine, computer network operations (CNO) are a component of Information Operations and break down into computer network defense (CND), computer network exploitation (CNE) and computer network attack (CNA). (Joint Publication 3-13)

While the main purpose of CND and CNA is self-evident, CNE is somewhat more controversial. It primarily refers to covert intelligence gathering, but it is unclear where the ‘exploitation’ ends and the ‘attack’ starts. From the defender’s perspective, it is very difficult to tell if an intrusion into their systems is an attempt to gather military intelligence (CNE), to prepare for a subsequent attack (CNA), to make money (criminals), or to make an ideological statement (hacktivist).

Of the three, CND is the most mature discipline. This does not mean that the art of defense is perfected - just that know-how is available and widespread. The offensive forms of operations (CNE, CNA) are comparatively rarely discussed in public and the actual capabilities of various actors are difficult to assess. It is this emergent quality that raises offensive cyber operations into the hybrid threat discussion.

The western doctrine is by no means finalized, nor is it the only one. For example, the Chinese military has spent nearly two decades of developing 'informationized warfare'. Inspired (shocked) by the US performance against the Soviet style forces of Iraq in the Gulf War, Chinese scholars and military leaders have blended the techno-centric approach of the US doctrine with the ancient 'Art of War' of China. (See, for example, Thomas 2007, 2009) The resulting mix offers a potentially more holistic approach than the often stove piped and limited Western IO doctrine.

The Russian military doctrine (or vision) of the future wars also combines conventional and unconventional approaches. For example, there is strong emphasis on the question of information superiority, both in terms of functionality of systems and of the prevailing content or narrative in the information sphere and the public perception. There is also discussion of using unconventional concepts like nano technology weapons, 'disorganization' techniques, affecting people's thought processes, etc. (See Thomas 2011 for more details) While it is unclear how much and which components of the unconventional approach are mere intellectual musings, it is a strong indication that Russia should be considered as a hybrid actor.

Another view of cyberspace is focused on the opportunities offered by cheap and easily accessible computing devices and global networking. Online shopping, social networks, strong public cryptography and (anonymous) real-time communication are examples of this. These solutions provide asymmetric advantages to actors who have limited resources. For example, it is possible to raise awareness of an issue on a blog, find people who are supportive of the cause through social networks and coordinate group actions on encrypted chat channels. On the other hand, the technology also allows for much greater control by those in power. For example, state (security) services might limit people's access to the Internet or specific services, eavesdrop unencrypted (or weakly encrypted) communications and even hack into personal computing devices to gather evidence against them.

The possibility to perform these activities with scarce resources enables sub-state actors. This is a big change compared to the Cold War and earlier times. The hacktivist group Anonymous has reported, for example, that its members recently hacked several hundred websites and published information on thousands of Israeli government officials as a response to Israeli efforts to shut down Internet in the Gaza Strip (see Figure 1). (RT.com 2012) This is a non-state actor attacking a state, as in the case with Hezbollah during the Lebanon war (although the scenario was quite different). Israel's finance minister declared in no uncertain terms that the government was now waging war on a "second front" [in cyberspace]. (RT.com 2012)

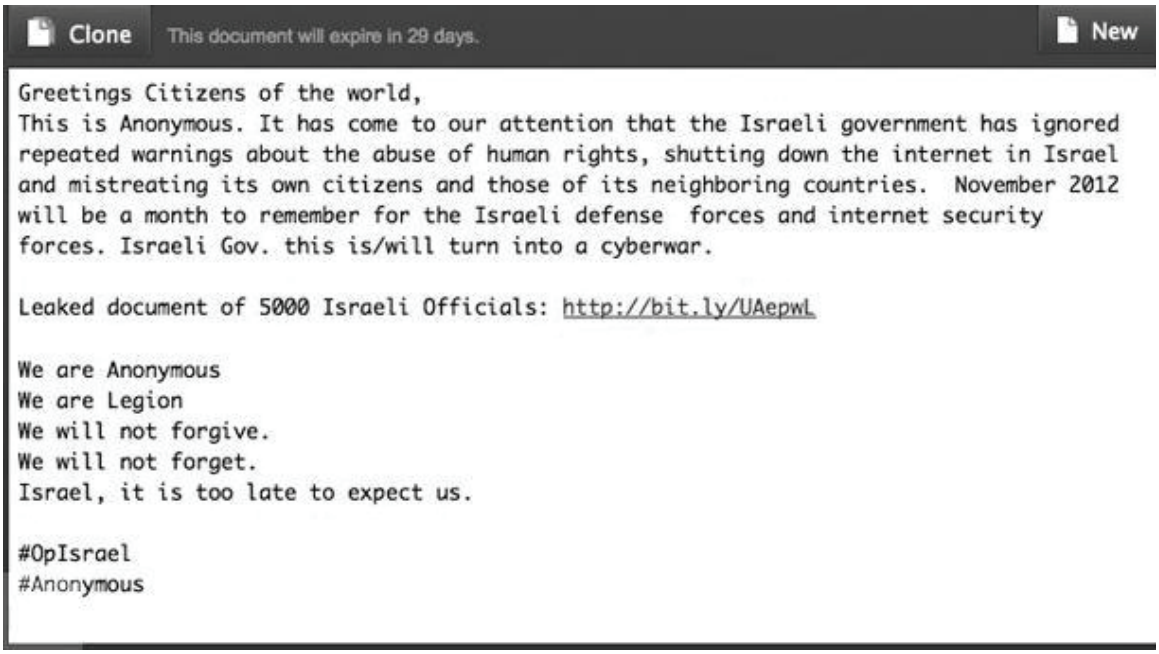

Figure 1: A message from the hacktivist group Anonymous (RT.com 2012)

The war-like reference might seem a bit overdone, but cyber operations against a state are likely to get such reactions, depending on how serious the state thinks the problem is. A US state official has stated that "If you

shut down our powergrid, maybe we put a missile down one of your smoke stacks". (Gorman and Barnes 2011)

Cyberspace is a contested environment. In recent years there have been many interesting developments to illustrate this point. The discovery of the StuxNet malware in 2010 created a lot of discussion about government malware and sabotaging critical infrastructure through cyber-attacks. (See, for example, Falliere, Murchu and Chien 2011, Sanger 2012, The Economist 2010a) In Germany, a debate sparked on the use of malware and hacking techniques for law enforcement purposes. (See, for example, Herkner 2007) The so-called Arab Spring demonstrated the dual use of information technology for both the people and the government. (See, for example, Afanasjev 2011)

The international community is trying to find consensus on some of these issues, but so far there is little success. There are efforts to shape or analyze the legal instruments for this area, such as the Council of Europe Convention on Cybercrime (2001) or the Tallinn Manual on the International Law Applicable to Cyber Warfare (2013). In reality, however, state practice is developing the norms for tomorrow.

4. Overlap of cyberspace (operations) and hybrid threats

From the perspective of hybrid threats, cyberspace can be viewed in several ways. First, cyber capabilities in support of conventional forces. Second, as an asymmetric and unconventional attack vector on its own. Third, as an enabler or disabler of events and social movements.

4.1 Supporting conventional forces

Offensive cyber capabilities may one day be considered part of the 'conventional' toolkit. However, for now they are a rarity in military combat operations and can be safely categorized as 'unconventional'. This means that any military operation that includes offensive cyber operations as well as conventional capabilities is by definition a manifestation of hybrid threats. Potential targets of military cyber attacks include sensors, computer controlled systems (drones, guided missiles, etc.), command, control, and logistics systems, etc.

Remotely controlled or autonomous drones operating in air, land, sea or space domains, rely completely on computers and computer networks to function. As such, they also fall into the domain of cyber operations. An interesting example of a possible cyber attack against such systems occurred in 2011, when Iran was able to manipulate a US drone to land in Iran - in effect, performing a remote hijack of the drone. While technical details are not published, there is speculation that the event involved jamming the control signal (forcing the drone into autopilot mode), as well as jamming and spoofing the GPS signal (tricking the drone into landing at the wrong coordinates). (See, for example, Peterson 2011; Rawnsley 2011)

It is important to note that the cyber operation does not have to cause lasting effects. For example, a short disruption in adversary air defense sensors or control systems may be the only goal of a cyber operation that is preceding an air strike. A potential example of such an event is the Israeli air strike against the alleged Syrian nuclear site in 2007, where Israeli (non-stealth) planes flew the mission without being harassed by Syrian air defense. Potential explanations include built-in kill switches in the Syrian systems or advanced EW capabilities. (See, for example, Adee 2008; Fulghum 2007)

However, the most likely target for military cyber operations is not a drone or any other tactical weapon system. The modern military relies heavily on its logistics and communication systems. These systems are more vulnerable to cyber attack, since they are less mobile and less reliant on custom hardware and software (compared to a drone, for example). Consider the strategic and operational effects of a cyber attack that scrambles the data (in a way that is not easy to restore) in the information systems of a major logistics hub: which container is where, what is in that container, who needs what, when they need it, etc. At the very least there will be delays, which could translate into loss of tactical or operational momentum and lives.

The military must be able to protect their own systems from cyber attacks. However, in many instances the military is reliant on or sharing infrastructure (dual use systems) with non-military systems, such as civilian Internet Service Providers. Therefore, the military must also be concerned with the security of these enabling systems. The problem here is that the military is rarely in a position to actively contribute to their defense. The

best approach is to map the dependencies and mitigate the associated risks through cooperation and duplication of service providers.

4.2 Non-military targets

A hybrid actor might also target systems that are not directly linked to the military. It is important to note that such attacks could be in violation of international law, depending on the circumstances. However, there are actors who are not (too) concerned with laws, so it makes sense to explore this from cyber hybrid threat perspective. While the military is typically not responsible for the protection of these systems, it is important to realize that attacks against them can significantly change the conditions that the military has to operate in. For example, an attack against civilian infrastructure could cause civil unrest or a mass evacuation in the area of operations.

If an actor wanted to influence the state or the population in general, then an obvious (although probably unlawful) target would be some Critical Information Infrastructure (CII) system. Our societies and economies are very dependent on CII, which are the information systems that enable and maintain our way of life. For example, systems that are used to control the power grid, water treatment plants, air traffic control and banks. In recent decades, critical infrastructure has become more and more automated in order to increase efficiency. Often this has also increased the attack surface of the information systems within.

CII attacks, if successful, could cause serious harm to human life, (critical) infrastructure, economy, ecology, etc. While most of this is hypothetical so far, it is within the realm of the possible. StuxNet is a great example of a cyber attack that causes physical damage against critical infrastructure. It is exceptional, because it exploits four zero-days (vulnerabilities that are only known to the attacker), disrupts industrial control systems and damages physical devices. While nobody has taken responsibility for the attack, there is general consensus that it was developed and deployed by a state or states. It manipulates the parameters of the variable frequency drives (programmable logic controllers - PLCs) that control uranium enrichment centrifuges. This causes the centrifuges to speed up and slow down repeatedly and rapidly. The two primary effects are that the enrichment process is no longer efficient (the isotopes mix again when the centrifuge slows down) and that the centrifuge may physically break due to mechanical stress (the discs inside the centrifuge may shatter). (See, for example, Falliere, Murchu and Chien 2011, Sanger 2012, The Economist 2010)

The same approach can be used against other types of CII, since PLCs are used everywhere, from elevators to nuclear power plants. However, this does not mean that physical damage is always possible. First, there could be alternative systems or safeguards (for example, brakes on the elevator). Second, the system may not involve destructive forces (for example, banking systems deal with information). It is also clear that physical destruction is not the only outcome that has national security implications. An attack against the banking sector that leads to bank runs can cascade into a serious economic problem for a state - more costly, perhaps, than a bomb.

However, CII is not the only concern when facing a cyber-enabled hybrid threat. Everyday life gets more and more entangled with information technology enabled services and devices. Consider, for example, that your smart phone 'knows' your location, schedule, contacts, etc. If soldiers take their smart phones to the field, they and their units can be tracked in real time by technologically savvy adversaries.

But information technology is becoming even more intimate. There are medical devices that are surgically implanted into people - pacemakers, insulin pumps, etc. The problem is that those devices are sometimes very poorly secured. Researchers have been able to remotely manipulate such devices (in lab conditions) in ways that could kill or harm a person. (See, for example, Halperin et al. 2008; Kirk 2012) While there are no known examples of lethal attacks against personal cybernetic enhancements, they should be considered in case a key person has one 'installed'.

With this in mind, it is clear why a hybrid threat actor might consider offensive cyber operations against non-military targets - the list of potential victims keeps growing and very often these systems are not hardened against dedicated attackers. While the military is not the right entity to provide security for these systems, they may be in charge of disabling or eliminating the source of the attacks. In addition, the military should be

ready to provide assistance to local crisis management services, upon request and within the existing legal framework.

4.3 Environment

The third reason to consider cyberspace from the hybrid threats perspective is that it offers new ways of accomplishing tasks that were previously prohibitively expensive or complicated. For example, consider the challenges of global communications and self-organization under oppressive regimes before the widespread adoption of Internet.

While cyberspace did not provide the motivation for the so-called Arab Spring, it definitely had a role in the events. On one side, people used the Internet to gather and share information about their governments, and to self-organize using social media and instant communication tools. On the other side, several governments tried to limit access to the Internet or to specific services on the Internet in order to regain control and to quell the unrest. (Afanasjev 2011)

It is well known to the national security and intelligence community that terrorist organizations use cyberspace to facilitate their operations. The Internet provides accessible, cheap (free) and anonymous ways to spread propaganda, identify and shape recruits, share training materials, gather intelligence, plan and coordinate attacks, etc. (Bardin 2010) However, to date there are no publicly known cases of cyber terrorism - cyber attacks that aim to coerce a population or government through terror.

Criminals and criminal groups are also taking advantage of cyberspace. Identity theft (including theft of credit card information), fraud, money laundering, extortion (for example, by using ransomware that encrypts the victim's data, or by performing distributed denial of service attacks), sale of counterfeit goods, and breaking into bank and electronic currency accounts are just a few examples of criminal use of cyberspace. The relative anonymity and problems with international law enforcement cooperation foster a thriving underground community that operates on a global scale.

Cyberspace is also a useful medium for espionage. Since the vast majority of information is stored digitally, the cyber spy can usually operate remotely. This means that there is very little risk of getting caught (although one might be identified), especially considering that there is no international law prohibiting espionage. From the hybrid threats perspective it allows to even the playing field considerably by 'skipping' the research and development phase on new technologies or by getting advance warning of deployments and capabilities of adversaries.

Intelligence agencies are actively monitoring Internet in the interest of national security. This is a rather passive and defensive form of cyber operations compared with cyber attacks. Still, the signs are clear that many states are preparing for cyber conflict. What we can conclude is that cyberspace is an area of conflict where states act in an apparently more direct way than they would when it comes to conventional means. Getting peoples' and organizations' financial information or destroying uranium enrichment centrifuges in conventional ways would stir up a lot more controversy than it does in the cyber world – much because the problems with attribution. The old definition of hybrid threats that non-state actors wield state actor capabilities seems to be in reverse here, as state actors try to masquerade as non-state actors. There are most likely a host of reasons for this, but again – the lack of strong attribution is a key enabler.

Cyberspace in itself can also be attacked with rather conventional means. Consider the problem of supply side vulnerability. In recent years there have been numerous cases of counterfeit microchips and other hardware, which could also contain hidden flaws, back doors or remote kill switches. National security is at risk as modern missiles, airplanes, and even munitions often have microchips in them. In the future one can imagine nanotechnology applied undercover on sensitive hardware, which might result in faulty or even changed functionality.

Once again, the military is not the primary actor in this field. However, it is very important to stay informed of the opportunities that information technology provides and to embrace them where applicable. In terms of social media, the military must practice good OPSEC on one hand, and STRATCOM on the other hand. For

example, NATO homepage has links to the Alliance's presence on FaceBook, Twitter and YouTube, in order to reach the demographic that prefers this type of media. (Newsroom 2013)

5. Conclusion

The national security implications of cyberspace are growing. Many states have recognized the importance of being able to operate in cyberspace – if for nothing else, then to boost their economy. Some states have even started developing military capabilities to ensure freedom of action during military conflicts, while suppressing the adversary's capabilities. It is also widely believed that state actors are very active on the cyber espionage front, although this is done in a clandestine manner.

This new focus on cyber capabilities is mirrored by sub-state actors as well. From individual activists to organized crime to terrorist organizations, these actors are seeking ways to benefit from cyberspace. On the one hand this is about using the myriad services available: communication, information gathering, etc. On the other hand, it is about abusing the services – harvesting personal information, stealing money, disrupting other services, etc. Traditionally, this form of activity has not been of much interest for the military. On the modern battlefield, however, cyberspace enables both prospective allies and enemies, engages the global community with local operations, and creates new modes of operating for the military.

For (relatively) like-minded states, such as members of NATO and EU, it is important to develop a common understanding on the opportunities and risks posed by cyberspace. On the defensive side, international cooperation is required to deter or defeat serious cyber threats, whether military or not. Cooperation between military and civilian (government and private) sector sphere is also required, since most of the CII is not owned and operated by the military, but may impact the capability or operations of the military. Therefore, the military must be ready and eager to cooperate and share with various partners that also have 'cyber power' and can affect the mission.

Acknowledgements

The authors would like to thank the Swedish National Defence College for funding this work.

References

Adee, S. (2008) "The Hunt for the Kill Switch", *IEEE Spectrum*, May. Available at: http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch/0. [Last accessed: 13.02.2013]

Afanasjev, M. (2011) *Approaches to Avoiding Government Censorship, Blockade and Surveillance on the Internet*. Master's thesis, Tallinn University of Technology.

Bardin, J. (2010) *Cyber Jihadist Use of the Internet: What Can Be Done?* Whitepaper.

Council of Europe. (2001). Convention on Cybercrime. Available at: http://conventions.coe.int/treaty/en/treaties/html/185.htm. [Last accessed: 13.02.2013]

Falliere, N., Murchu, L.O. and Chien, E. (2011) W32.Stuxnet Dossier. Available at: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. [Last accessed: 13.02.2013]

Fulghum, D. (2007) "Why Syria's Air Defenses Failed to Detect Israelis", *Aviation Week*, Oct 3. Available at: http://www.aviationweek.com. [Last accessed: 13.02.2013]

Gorman, S. and Barnes, J.E. (2011) "Cyber Combat: Act of War. Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force", Wall Street Journal, May 30. Available at: http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html. [Last accessed: 13.02.2013]

Halperin, D., Heydt-Benjamain, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T. and Maisel, W.H. (2008) "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses", *Proceedings of the 2008 IEEE Symposium on Security and Privacy*. Available at: http://www.secure-medicine.org/icd-study/icd-study.pdf. [Last accessed: 13.02.2013]

Herkner, L. (2007) "Hacken für den Staat", Zeit Online, May 16. Available at: http://www.zeit.de/2007/21/Sicherheitsplaene. [Last accessed: 13.02.2013]

Ho, J. (2005) "The Advent of a New Way of War: Theory and Practice of Effect Based Operations", Johan Elg (Ed.), *Effektbaserade operationer,* Stockholm.

Joint Publication 3-13. Information Operations. (2006) Chairman of the Joint Chiefs of Staff.

Kirk, J. (2012) "Pacemaker hack can deliver deadly 830-volt jolt", ComputerWorld, Oct 17. Available at: http://www.computerworld.com/s/article/9232477/Pacemaker_hack_can_deliver_deadly_830_volt_jolt. [Last accessed: 13.02.2013]

Markoff, J. (2008) "Before the Gunfire, Cyberattacks", NYTimes.com, Aug 12. Available at: http://www.nytimes.com/2008/08/13/technology/13cyber.html?em&_r=0. [Last accessed: 13.02.2013]

Matthews, M.M. (2008) "We Were Caught Unprepared: The 2006 Hezbollah-Israeli War", *The Long War Series Occasional Paper 26*. U.S. Army Combined Arms Center, Combat Studies Institute Press, Fort Leavenworth.

Mattis, J. (2008) "Commander's Guidance for Effects-Based Operations", *Joint Forces Quarterly,* 51:4, Washington.

Newsroom (2013) North Atlantic Treaty Organization. Available at: http://www.nato.int/cps/en/natolive/index.htm. [Last accessed: 13.02.2013]

Peterson, S. (2011) "Exclusive: Iran hijacked US drone, says Iranian engineer (Video)", Christian Science Monitor, Dec 15. Available at: www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video. [Last accessed: 13.02.2013]

Rawnsley, A. (2011) "Iran's Alleged Drone Hack: Tough, but Possible", Wired, Dec 16. Available at: http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps/. [Last accessed: 13.02.2013]

RT.com (2012) "Anonymous leaks personal information of 5,000 Israeli officials", Nov 18. Available at: http://rt.com/news/anonymous-israel-officials-leaked-002/. [Last accessed: 13.02.2013]

Sanger, D. (2012) "Obama Order Sped Up Wave of Cyberattacks Against Iran", NYTimes.com, June 1. Available at: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&pagewanted=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all. [Last accessed: 13.02.2013]

Tallinn Manual on the International Law Applicable to Cyber Warfare (to appear 2013). Cambridge: Cambridge University Press. Draft available at: http://www.ccdcoe.org/249.html. [Last accessed: 13.02.2013]

The Economist (2010a) "A worm in the centrifuge", Sep 30. Available at: http://www.economist.com/node/17147818. [Last accessed: 13.02.2013]

The Economist (2010b) "War in the fifth domain", Jul 1. Available at: http://www.economist.com/node/16478792. [Last accessed: 13.02.2013]

Thomas, T. (2007) *Decoding the Virtual Dragon: Critical Evaluations in the Science and Philosophy of China's Information Operations and Military Strategy*. Fort Leavenworth: Foreign Military Studies Office.

Thomas, T. (2009) *The Dragon's Quantum Leap: Transforming from a Mechanized to an Informatized Force*. Fort Leavenworth: Foreign Military Studies Office.

Thomas, T. (2011) *Recasting the Red Star: Russia Forges Tradition and Technology Through Toughness*. Fort Leavenworth: Foreign Military Studies Office.

Wiener, N. (1948) Cybernetics: Or Control and Communication in the Animal and the Machine. New York: John Wiley.

Aapo Cederberg has a long career in the Finnish Armed Forces, lastly as Senior Military Adviser at the Permanent Mission of Finland to the OSCE in 1999- 2003, Commander of the Häme GBAD Battalion in 2003 – 05, Head of Strategic Planning at the Ministry of Defence in 2005 – 2007 and at present Secretary General for the Security Committee at the Ministry of Defence since 2007. The Committee supports the Government in comprehensive security matters and has provided the Security Strategy for the Society as well as Finland´s first Cyber security Strategy

Mini Track Chairs

Dr Nasser S. Abouzakhar is a senior lecturer at the University of Hertfordshire, UK. Currently, his research area is mainly focused on critical infrastructure security and applying machine learning solutions to various Internet and Web security and forensics related problems. He received MSc (Eng) in Data Communications in 2000 followed by PhD in Computer Sci Engg in 2004 from the University of Sheffield, UK. Nasser worked as a lecturer at the University Of Hull, UK in 2004-06 and a research associate at the University of Sheffield in 2006-08. He is a technical studio guest to various BBC World Service Programmes such as Arabic 4Tech show, Newshour programme and Breakfast radio programme. Nasser is a BCS assessor for the accreditation of Higher Education Institutions (HEIs) in the UK, BCS chartered IT professional (CITP), CEng and CSci. His research papers were published in various international journals and conferences.

Dr Rain Ottis is a scientist at the NATO Cooperative Cyber Defence Centre of E xcellence, in Tallinn, Estonia. He previously served as a communications officer in the Estonian Defence Forces, focusing primarily on cyber defence training and awareness. He is a graduate of the United States Military Academy (BS, Computer Science) and Tallinn University of Technology (PhD, Computer Science; MSc, Informatics). His research interests include cyber conflict, national cyber security, politically motivated cyber attacks and the role of volunteers in cyber security. In addition to his current assignment, he is teaching cyber security in Tallinn University of Technology (EST) and University of Jyväskylä (FIN).

Dr Aki Huhtinen is a professor at Finnish National Defence University. His expertise areas are military leadership, and philosophy of war.

Dr Jari Rantapelkonen is a professor at Finnish National Defence University. His expertise areas are strategic communication and operational art and tactics.

Biographies of Presenting Authors

Nasser Abouzakhar is a senior lecturer at the University of Hertfordshire, UK. Currently, his research area is mainly focused on applying machine learning solutions to critical infrastructure protection. He received PhD in 2004, the University of Sheffield. Nasser is a BCS assessor for the accreditation of Higher Education Institutions in the UK, CEng and CSci.

Kari Alenius is Associate Professor in the Department of History at the University of Oulu, Finland, since 1998. He also has Adjunct Professorship at the University of Oulu (1997). His research interests include the history of propaganda and mental images, the history of Eastern Europe between the World Wars, and the history of ethnic minorities.

Olga Angelopoulou, BSc, MSc, PhD is a lecturer and the programme leader for the MSc Computer Forensic Investigation at the University of Derby. She obtained a doctorate in Computing with the title: 'Analysis of Digital Evidence in Identity Theft Investigations' from the University of Glamorgan. Her research interests include Digital Forensics, Identity Theft, Online Fraud, Digital Investigation Methodologies and Online Social Networking.

Dr Edwin "Leigh" Armistead is the President of Peregrine Technical Solutions, which focuses on IO and Cyber Security. Leigh received his PhD from Edith Cowan University with an emphasis on IO, and serves as Co-Editor for the Journal of International Warfare, plus the Editorial Review Board for ECIW and is the Programme Director for ICIW.

versity, Taiwan in 1997, and both a M.Sc. degree and a Ph.D. (Computer Science and Engineering) from National Sun Yat-sen University, Taiwan in 1999 and 2010, respectively. His research interests include Internet security, wireless network, home network system, IoT, and learning cloud services.

Eric Filiol is the head of the Operational Cryptology and Virology at ESIEA. He has spent 21 years in the French Army. He holds an Engineer diploma in Cryptology, a PhD and a Habilitation Thesis in applied mathematics and computer science. He is also the Scientific Director of EICAR and the Editor-in-chief of the Journal in Computer Virology.

Jason Flood, MSc is currently an Ethical Hacking Architect at IBM in Dublin. He is also a PhD student at the Institute of Technology Blanchardstown where he investigates better ways of training Network Administrators. Jason is the co-founder Irish Chapter of the Honeynet Project and works with OWASP and Facebook in running CTF competitions.

Grigorios Fragkos, BSc, MSc, PhD, Certified TigerScheme, AST and QSTM. He has a number of publications in Computer Security and Computer Forensics. He has been part of the CyberDefense dept. of the Hellenic Army acting as Information Security consultant and Penetration tester. Currently, works for Sysnet Global **Solutions as Sr. Consultant and Penetration tester.**

Wendy Goucher is about to enter the final phase of her PhD research. She is a part time student at University of Glasgow and is also an information security consultant with Idrach Ltd. where she specialises in assisting in the design and communication of operationally effective security policy.

Dijana Grd comes from Croatia. She is a second year student of graduate study programme Information and Software Engineering at Faculty of Organization and Informatics in Varazdin. Her studies have provided her an insight into area of identification, collection, processing, analysis and production of electronically stored information. She has some work experience as a student assistant in Informatics and as a project manager in student organization AIESEC. She enjoys participating in all kind of international conferences and projects. She also likes to travel and meet new people.

Clement Guitton is a PhD candidate in War Studies at King's College London focusing on cyber security. He holds a master degree both in international relations and in electrical engineering. Fluent in English, French, and German, he previously worked at the International Telecommunication Union, the United Nation agency specialised on information and communication technologies.

Håkan Gunneriusson has a PhD in History 2002, Uppsala University. Hakan is interested in sociological and historical perspectives on current and coming issues regarding military tactical and cultural issues. Hakan is currently head of research ground operative and tactical areas, Swedish National Defence College.

Samuli Haataja is a PhD candidate in the Griffith Law School at Griffith University on the Gold Coast, Australia. He holds a Bachelor of Laws (Hons) and Bachelor of International Relations from Griffith University. His research focuses on cyber attacks and international law – specifically on the relationship of technology, violence and law in this context.

Mikko Hakuli is currently employed as security specialist at JyvSecTec-project in Jyväskylä University of Applied Sciences (JAMK), where his main responsible are technical security testing and development of various situational awareness "best practices" in cyber-security area. Formerly he worked as Head of information security on Finnish Airforces. Currently he also make studies in University of Jyväskylä and Jyväskylä University of Applied Sciences.

Juhani Hämäläinen received his PhD degree in theoretical physics from the University of Jyväskylä in 2004. He is currently in the position of principal scientist at Finnish Defense Forces Technical Research Centre (PVTT). His research interests include mathematical model development and operational analysis.

Major Arto Hirvelä is an instructor (leadership) in a research group at the Finnish National Defence University. He is preparing a doctoral dissertation in Military Science (leadership). His research interests are information environment, strategic communication, and information operations.

Ilona Ilvonen is a doctoral student at Tampere University of Technology, department of Information Management and Logistics. Her doctoral thesis topic is the management of knowledge security, and the thesis is due in 2013. She has published conference papers on information security management, knowledge management and relating topics since the year 2003.

Margarita Jaitner is a research intern at the Finnish National Defence University. She received a Bachelor's degree in Political Science at the Swedish Defence College and is currently pursuing a Master's degree in Societal Risk Management at the Karlstad University in Sweden.