CICERO FOUNDATION GREAT DEBATE PAPER

No. 12/08

December 2012

THE ROLE OF ESTONIA IN DEVELOPING NATO'S CYBER STRATEGY

HÄLY LAASME

Foreign Policy and Security Analyst

Estonia

Cicero Foundation Great Debate Paper No. 12/08

The Cicero Foundation is an independent pro-Atlantic and pro-EU think tank.

www.cicerofoundation.org

The Cicero Foundation

FRANCE

13, rue Washington

75008 PARIS

Tel. +33 1 45 62 05 90

Fax +33 1 45 62 05 30

Email info@cicerofoundation.org

THE NETHERLANDS

Hondertmarck D 45

6211 MB MAASTRICHT

Tel. +31 43 32 60 602

Fax +31 43 32 60 828

cicerofoundation@gmail.com

CONTENTS

THE ROLE OF ESTONIA IN DEVELOPING NATO'S CYBER STRATEGY

HÄLY LAASME[1]

"Yes, we must, indeed, all hang together, or most assuredly we shall all hang separately."
Benjamin Franklin[2]

Introduction

Benjamin Franklin, one of the Founding Fathers of the United States of America, had an ideal of Britain and America flourishing together in the global community, but then he realized that independence was the only way out of the subjugation problem of colonies. Nevertheless, Benjamin Franklin's hope for unity was realized roughly 200 years later, on April 4, 1949, when the North Atlantic Treaty Organization (NATO) was founded. However, he probably would never have imagined the unification of 28 sovereign states under one Treaty in an attempt to preserve their security, peace, and freedom. Considering the violent history of humanity, it seems that the global community often underestimates the accomplishments of NATO that in a not so distant future might, eventually, become a century-old Alliance. Contrary to the highly skeptical view of neo-realists as concerns the significance of international organizations[3] as a deterrent to war, NATO has proved that, even though the formation of an effective strategy might often seem to be an illusion, it is a necessary organization for achieving common security and peace.

However, a strategy can fail if the means that have been chosen prove to be insufficient to the ends.[4] NATO's objectives are the preservation of peace and security while maintaining the principles of democracy, individual liberty, and the rule of law.[5] In 1949, the drafters of the Treaty, who wanted to build a collective defense mechanism in order to assure these objectives, could possibly not have foreseen the evolution of modern society where the conventional domains of land, sea, and air, were enlarged with a space dimension and new, hybrid combinations of man and technology would revolutionize warfare in a 'info-bio-nano-robo-hydro-cogno' society in which the collective defense should be realized within the predicaments of Moore's Law.[6]

Fortunately for the Allies, NATO has survived all scientific revolutions of the previous sixty years. It has emerged stronger than ever despite the realists' ominous predictions of the last decade that the Alliance would dissolve and lose its purpose. The post-Cold War enlargement of NATO that was feared to exhaust its existing members seems to have actually strengthened the Alliance by forcing it to leave the static mindset and become more dynamic, by giving it a fresh purpose and transforming it to a more coherent structure. Even if it might appear that there is no need for such an ambitious defense alliance in the predominantly peaceful contemporary world, NATO's survival is imperative in order to face ever more complex emerging challenges that necessitate collaborative efforts and cannot be solved by any transatlantic country alone. Therefore, some of the Allies have vigorously promoted NATO's development and its reinvention into a two-fold actor, provider of collective defense and of collective security.[7] As a matter of fact it is the evolution of the cyber domain that has exponentially increased our society's reliance on digital and electronic infrastructure and made NATO Allies and Partners realize that they all have to "hang together" to face the future or they "most assuredly shall hang separately."

To better comprehend the evolution of NATO's cyberpower, this paper has been divided into three parts. The first part will describe how and why the new Ally, Estonia, became the catalyst of NATO's Cyber Policy. The second part will analyze the developments in NATO's Cyber

Strategy and the third part will discuss the preparedness of the Alliance to face the emerging challenges. In addition, this paper will ask attention for some issues that have been less discussed in most of NATO related literature.

PART I – The Unexpected Catalyst.

Estonia as an 'e-State'

The significance of small states within multilateral fora is often underestimated and misunderstood because the focus is rather on power than on influence. In fact, small states have demonstrated that they are capable of acting strategically to preserve security while contributing to the stability and efficiency of international organizations.[8] In addition, smaller nations are more likely to launch initiatives that appear to be small contributions, but, in time, prove to be major developments.[9] Because these nations have a tendency to suffer from inferiority syndromes they are tempted to "show their mettle" by trying to excel in their initiatives.[10] In the case of NATO, Estonia in particular has demonstrated the relevance of the previous assumptions. Estonia, the birth-country of Skype and Keyless Signature Infrastructure,[11] is one of the smallest allies of NATO. By magnitude from smallest to largest, it is third in population, seventh in total area and in 2011 it was third in GDP (Table 1, Annex[12]). Between 2005 and 2010, Estonia was considered one of the leading countries in the utilization of digital and electronic infrastructure. For example, it ranked 2nd in the world after the United Arab Emirates (UAE) in mobile phone subscriptions where each person in Estonia owned at least one device on average - and in 2009 it was 18th in Networked Readiness Index among 134 countries.[13]

Although many of the Allies have significantly advanced their civil electronic capabilities since 2005, Estonia has been continuously considered as part of a digital elite that apart from positive advancements is also capable of demonstrating the negative consequences of increased digital

awareness among the population.[14] In the 2012 Security & Defence Agenda Report, Estonia scored in the cyber security stress test at the same level as Denmark, France, Germany, the Netherlands, Spain, United Kingdom (UK), and United States (US).[15] According to the 2012 Networked Readiness Index, Estonia holds the 24th place among 142 countries. Within NATO, Estonia ranks 12th overall and 1st in the Social Impact Pillar (10th Pillar) that measures improvements in the well-being of citizens driven by Information and Communications Technologies (ICT) (Table 2, Annex[16]). In Estonia, daily life is characterized by hyper-connection, using various mobile technologies and digital innovations, such as e-government and e-Cabinet, e-voting, e-parking, e-banking, e-ID system, e-taxes, e-police, e-prescriptions, electronic health records, digital signing, live-streaming public TV, etc.[17] Briefly, Estonia has attempted to realize anything that it could possibly do by utilizing digital infrastructure, with the aim to make its tiny society more efficient and sustainable under budgetary and demographic constraints. Therefore, in Estonia, access to the internet is considered as a basic human right, because it is an essential utility to its citizens for acquiring democratic freedoms.[18] On the other hand, the increasing dependence on technology to sustain society has made Estonia extremely vulnerable to a myriad of security risks and consequently forced the country to become a driving force of NATO's Cyber Defense Policy.

Attack on e-Estonia

In February 2006, the US conducted the first full-scale cyber security exercise called "Cyber Storm" that simulated a malicious large-scale cyber incident affecting or disrupting multiple critical infrastructure elements, including information technologies of government.[19] In April 2007 this scenario became a reality for Estonia when during a three-week period its servers and routers became victims to patriotic hacking from approximately one million computers from 178 countries.[20] The attacks started after government had officially started working on the relocation of the Bronze Soldier, a Soviet WWII memorial, and war graves, to a military cemetery by fencing and covering the memorial site on 26 April. At the same night the Estonian capital was the theater of political riots, mostly by ethnic Russians, which turned into an

emotional outpour in the cyber domain by 27 April. From that day on the attacks became increasingly more sophisticated and coordinated and at their peak the internet traffic targeting Estonian government sites was almost 400 times above the normal traffic rate. Among other methods, the attackers utilized huge botnets for distributed denial of service (DDoS) attacks, defaced the website of the Estonian Reform Party and disrupted domain name system (DNS) services in parts of the country.[21] To mitigate the consequences to national security, the Estonian information technology (IT) managers had to block the international connections to the servers, which created a situation akin to a modern blockade of a country without concomitant deployment of any conventional weapons.[22]

Even though Estonian officials and citizens believe that the cyber attacks on Estonia were supported by the Russian government, the latter has denied any official involvement in the incident and refused to cooperate with the Estonian investigations into this matter.[23] Ex post, the magnitude of the incident brought an overwhelming international attention to the inadequacy of the legal frameworks for the cyber domain, especially in the cross-jurisdictional environment, and to the deficiencies of technologies for mapping attribution.[24] Consequently, cyber experts have concluded that even though the Estonian incident was a first serious full-scale cyber attack on the nation state, it could not be considered as a state-sponsored attack. It could best be classified as a level 1 attack according to the AF-SAB/US military model.[25] The scale and consequence threshold of the cyber attacks on Estonia did not constitute armed attacks[26] that would have invoked Article V of the North Atlantic Treaty.[27]

Innovative Approach to Cyber Defense and the Abolition of Free Riding

After the 2007 cyber conflict, Estonian diplomatic skills quickly surpassed many of its peers as it became the leading promoter of international cyber security in NATO and the EU.[28] In addition, an Estonian proposal, made in 2003, to create a Cooperative Cyber Defense Centre of Excellence (CCDCoE) in Tallinn, finally received strong support from NATO and in October 2008 it became a fully accredited international military organization.[29] Furthermore, to defend its electronic

infrastructure, the Estonian government resorted in 2011 to an innovative solution that was first proposed in 2007 and had not been utilized in any other democratic country. It officially established the Cyber Defense League under the all-voluntary home defense guard/Total Defense League, which resembles the concept of the Army National Guard in the USA.[30] This cyber reaction force is constituted of both civilian and military IT experts and cyber specialists who can be mobilized under paramilitary command for national security missions, such as defending critical electronic infrastructure. In addition, the Estonian government has taken even a further leap into the future by considering the possibility of a draft for cyber experts that would be available in case of national contingencies.[31] The idea behind this kind of strategy is actually quite straightforward. The majority of the best programmers and cyber experts work in the private sector which can offer them better opportunities for advancement and development. By joining the Estonian Cyber Defense League they are pledging to increase their knowledge and skills during peace time and utilize them for the benefit of the nation during a crisis.

However, there have been some opposing arguments against the conscription of private sector employees for this defense strategy, because it might have unintended economic consequences by disclosing proprietary information to competing business partners.[32] Nevertheless, the Estonian government is determined to do whatever it deems necessary to protect the nation's electronic infrastructure from future cyber attacks. After having developed their own comprehensive cyber security strategy in 2008,[33] the Estonian leaders were among the biggest critics of the EU and other European states which have not developed or implemented their cyber strategies for the defense of critical infrastructure.[34] What seems to concern Estonians most is not so much the cyber strategy per se. This is the structured combination of Ends (objectives), Ways (concepts/courses of action/methods for accomplishing ends), and Means (resources, elements of power, assets, capabilities). What does concern them is the lack of good cyber strategies that don't only provide "blue sky objectives while skipping over the annoying fact that no one has a clue as to how to get there."[35] The good cyber strategy has not only to

define what to accomplish but also how to accomplish it and with what resources.[36] Estonians expect it also to include a fairly transparent timeline.

Even though Estonians might seem alarmists to some Allies, their security concerns seem to be justified according to the Visegrad Group's (V4)[37] 2012 internal cyber analysis that emphasizes the cyber commitments that the Czech Republic, Hungary, Poland, and Slovakia have made, but failed to muster the political will for following through.[38] In addition, a geopolitically extremely important NATO Ally, Turkey, also seems to struggle with defining its cyber strategy and how to coordinate its fragmented cyber efforts under a more coherent umbrella.[39] At the same time, the UK does not only have a quite detailed Cyber Security Strategy[40] but it promotes its Defense Industrial Base (DIB) to pursue cyber-technologies that can assure national security[41] and it seem to have opted to forego the production of fully operational aircraft carrier for the benefit of expanding and maintaining its cyber capabilities.[42] However, Estonian officials believe that the cyber security of NATO and Europe is as strong as its weakest link and free riding should not be allowed. Consequently, they relentlessly pursue the development of a more coherent cyber strategy on an international level.[43]

Cyber attacks on Estonia are often described as a true wake-up call[44] or impetus[45] for NATO because they forced the Alliance to change its security trajectory into a more comprehensive approach by extending the development of cyber capabilities also to its members. [46] However, taking into account that some of the Allies had already realized their weaknesses in cyber security before the 2002 Prague Summit, the question should not be how Estonia became the driving force of Cyber Policy in NATO, but why it took the Alliance almost thirty years to develop and implement a Cyber Policy and the corresponding strategies.[47]

PART II – From Cuckoo's Egg to Willy Wonka.

NATO's Struggles and the Allies' Blindness

Looking back at the Estonian 2007 cyber conflict, as a matter of fact the actions of the Russian patriot-hackers proved counterproductive to the Russian foreign policy strategy that has always considered NATO and its enlargement as a threat to its sphere of influence in the region. Instead of increasing the Russian grip on Estonia, the event had unexpected positive consequences for the Alliance. Realists frequently argue that Alliances only survive when their members perceive a common threat.[48] In fact, these cyber attacks evoked a common threat perception among the Allies who had become quite disunited over the wars in Iraq and Afghanistan.[49] During the 2004 Istanbul Summit, NATO had to bridge deep strategic divisions between its members. By 2007 the Alliance was strained by Jacques Chirac's Gaullism and the strict guidelines for Bundeswehr operations, while some NATO members blocked the deployment of missile batteries to Turkey, and Dutch forces were reluctant to engage in combat operations.[50] Thus, the Alliance desperately required a new focus, which hackers provided in the form of the Estonian cyber incident. It drew Allies slowly back together. They started to debate, conducted joint exercises, and organized conferences and meetings on cyber security. Consequently, by finding a common threat that was relevant to all of them, the cyber issues managed to transform NATO to a more coherent and robust multilateral actor.

Unfortunately, this new found solidarity soon revealed a darker side of international bureaucratic institutions: the incapability to stay ahead of emerging challenges. As Jason Healey emphasized: "the blindness to history has immediate operational implications…. The longer we think cyber conflict is new, the more we will repeat the same mistakes and relearn old lessons."[51] Hence, it remains puzzling why it did take the Alliance more than two decades to realize the necessity to develop a comprehensive cyber strategy. Looking at the cyber heritage of the Allies, the policy should have been developed and implemented already before the second enlargement of NATO, which included Estonia. The US had its first serious cyber

incident, nicknamed "Cuckoo's Egg"[52] already in the 1980s. It was the 1986 international espionage case by Hanover Hacker, who compromised a multitude of computers, including military, in search of classified materials about the US Defense Strategy. In 1994, Rome Labs, the Air Force C2 (command and control) research facility in New York was compromised by Sniffer.[53] One year later the foundations were laid for the Information Warfare of the US Air Force and in 1996 the US Air Force established its first combat cyber unit, the 609th Information Warfare Squadron.[54] In 1997, the Joint Chiefs of Staff mandated to conduct an interoperability exercise, "Eligible Receiver", to test the Department of Defense (DoD) information infrastructure[55] and one year later a cyber incident, dubbed "Solar Sunrise", compromised the same DoD networks and computers.[56] In 1998, the Clinton administration published a White Paper outlining the Policy on Critical Infrastructure Protection and emphasizing the importance of protecting critical infrastructure from cyber attacks.[57] Hence, the US should have been highly aware of the vulnerabilities in cyberspace and know exactly where the Alliance had weaknesses, but for some reason the US did not propose the development of any comprehensive cyber strategy within the Alliance.

In 1999, during the Operation Allied Force (OAF) in Kosovo NATO networks and computers were attacked by pro-Serbian hackers for several days, which finally prompted the Alliance to implement the Cyber Defense Program at the 2002 Prague Summit. However, this program only concentrated on the defence of NATO's *internal* communication and information systems. This action of the Alliance came after the "I Love You" virus in 2000 that proved how easy it was to infect millions of computers,[58] and demonstrated that nobody should underestimate the success of spear phishing and social engineering which have become prevalent tactics for getting a foothold in today's cyber environment. As Martin Sadler has emphasized, cyberspace has its own ecosystems for organized crime and nation state operations, which include people with certain skills for different operations, such as conducting spear phishing, gathering information about who to attack, developing zero-days[59], operating and maintaining zero-days, marketing the service, etc.[60] The constant flow of new technologies and malicious techniques creates systemic vulnerabilities that are difficult to defend because a protection against a

certain kind of technique is almost outdated the moment it is introduced. Therefore, achieving 100% security in the cyberspace "is not only unrealistic but also results in a false sense of security"[61] and the cyber security investments should focus on areas that can produce significant negative consequences. This might be part of the reason why NATO hesitated so long as concerns the development of a comprehensive cyber security strategy and did not believe that the member states' networks were as relevant to its cyber security as its own. NATO ignored the basics of the information age, which, according to Kurt Herrmann, is secure and interoperable communication and information system (CIS) infrastructure because "connectivity is the prerequisite for successful political and military engagement."[62]

The Cradle of NATO's Cyber Policy and Smart Flag Waiving

Although the Alliance established the NATO Computer Incident Response Capability (NCIRC) as part of the Cyber Defense Program in 2002, it took the Alliance at least eight years to achieve full operational capability.[63] Hence, NATO seems to have had a retroactive perspective in cyberspace that only was transformed into a more serious proactive defense mode after the 2007 cyber attacks on Estonia, an effort significantly promoted by Estonian politicians. Finally in 2008, five years after the first US comprehensive cyber strategy,[64] NATO ratified its first Cyber Defense Policy and created the Cyber Defense Management Authority in Brussels.[65] To improve the Allies' cyber defense capabilities and interoperability, the tenth center of excellence (CoE), CCDCoE was established in the Estonian capital Tallinn, in May 2008, with a Memorandum of Understanding between Allied Command Transformation (ACT), the framework nation Estonia, and six other sponsoring members (Italy, Spain, Slovakia, Germany, Lithuania, Latvia).[66] Since 2008, the Netherlands, US, Poland, and Hungary have also joined the center. The aim of the K5, CCDCoE's preferred code name,[67] has continuously been to emphasize doctrine and concept development, awareness and training, research and development, analysis and lessons learned, and consultations relevant to the cyber domain.

One of the more imperative contributions of CCDCoE toward mitigating the impact of cyber conflicts has been the promotion of information sharing through annual International Conferences on Cyber Conflict since 2009.[68] In addition, to advance members' cyber defense capabilities, in May 2010, the CCDCoE organized together with the NCIRC the 13th NATO Cyber Defense Workshop and in October 2010 co-hosted with ACT a workshop "NATO in the Cyber Commons," which was strictly aimed at identifying the Alliance's vulnerabilities and developing relevant capabilities.[69] Meanwhile, the ACT workshop demonstrated exactly why NATO's actions in cyber domain lag behind some of its Allies. According to the report its participants believed that NATO has been "very quick in providing responses to the new paradigm on cyber security threats and maintaining awareness afterwards."[70] However, this was a far from reality to the people who know a little bit about cyber history and who believe that even more than a decade after the 1999 OAF incident NATO still has to catch up in cyber security.[71]

At the same time, it is vital to recognize that the capability of the CCDCoE in Estonia to contribute toward NATO's cyber strategy is limited, because CoEs are not part of NATO's command structure and not funded by the Alliance, although ACT coordinates and facilitates the dialogue between them. The CoEs are a supporting network of NATO by developing doctrines, improving interoperability, offering consultations, education and training, and collaborating in research and development. Therefore, the CoE's are actually the empirical examples of NATO's rebranded and renamed transformational agenda called "Smart Defense" that NATO Secretary General, Anders Fogh Rasmussen, has defined as "Ensuring greater security, for less money, by working together with more flexibility."[72] The primary aim of Smart Defence is to utilize the Allies' resources with more coordination and coherence and to encourage more collaboration in advancing their capabilities. However, the development of the CoEs, especially the CCDCoE in Estonia, has demonstrated that the contributions of the smaller countries can be sometimes as pertinent for the future of NATO as the significant financial and in-kind contributions of the bigger countries. Currently, there are 18 accredited CoEs, plus 3 in development, one in almost every post-Soviet Eastern European country[73] and without any doubt these are causing political headaches in the members of the Russian government. On the

other hand, to reap more constructive benefits from the CoEs, the hosting nations have to look beyond "flag waving", which is in itself, maybe a creative deterrent, but which is shortsighted without substance, and find ways to enhance cooperation between the participants and a diffusion of the results among all Allies and Partners.[74]

Toward the 2011 Cyber Policy

Since 2008 NATO has also conducted annually a Cyber Coalition Exercise. At first these exercises were limited to NATO entities, but since 2009 they have been open to all member states and even to the partner nations. It is a unique 3-day collaboration between the cyber specialists of NATO Headquarters and the national cyber defense facilities with the aim to strengthen cooperation and partnership between them. While these exercises require the teams to solve hypothetical crisis scenarios created by NATO in highly controlled environments, [75] some argue that NATO should implement even more realistic exercises. Similar arguments have been made about the USAF Aggressor Program where Airmen from the 57th and 177th (ANG) Information Aggressor Squadron infiltrate DoD networks.[76] During the 2011 International Conference on Cyber Conflict the idea of a so called NATO cyber red team was presented. Proponents argued that even though this approach could expose NATO temporarily to more risk, it would allow its teams to generate a more realistic assessment of the vulnerabilities and lead to the creation of more advanced cyber capabilities in the long term.[77]

Finally, after 24 years of struggling with the repercussions of the "Cuckoo's Egg" case for the Alliance, NATO decided to follow the recommendations of the group of experts[78] in the development of the new Strategic Concept. The 2010 Strategic Concept emphasized the importance of cooperative partnership in tackling the new emerging security challenges, including cyber security that was also captured within the NATO Capstone Concept of hybrid threat. "Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives." [79] The conceptualization of the hybrid threat finally shows NATO's acknowledgment of the cyber

age and that security threats against the Alliance's interests are no longer restricted by geographical limits, but that they can manifest themselves as complex threats that migrate through land, sea, air, and space, intertwining themselves through cyberspace. Deadly and devastating attacks against Allies can be perpetrated and initiated in an instant from remote locations, leaving no trail to determine their origin.[80] Therefore it is imperative that the Alliance follows through on expectations of the new Strategic Concept to develop a robust ability to not only prevent, detect, and defend against cyber attacks but also to recover from them if they prevail. To counter the cyber portion of the hybrid threats, the Alliance has taken its most significant steps during recent years, although it is lagging several decades behind its stronger Allies. For example, the 2010 Lisbon Summit Declaration, section 40, tasked NATO to prepare an in-depth cyber defense policy and an action plan for its implementation by June 2011.[81] Subsequently, NATO fulfilled this task by adopting a revised Cyber Defense Policy that included specific tasks that NATO should develop.[82] Attached to the Cyber Policy was an Action Plan that should guide the Allies in realizing their cyber defense objectives more specifically.

In addition, NATO has finally confronted concerns over the handling of cyber issues within its organization, although it might require more streamlining. At the highest level the oversight of the Cyber Policy is conducted by the North Atlantic Council. The NATO Cyber Defense Management Authority (NCDMA) coordinates and manages NATO's cyber defense capabilities. On the operational level, the Cyber Defense Management Board (NCDMB) coordinates the cyber defense efforts within the Alliance and receives expert advice and oversight from the Defense Policy and Planning Committee in Reinforced Format. On a tactical level, the activities are commanded by the Cyber Defense Coordination and Support Centre (CDCSC) in Brussels, while the technical and scientific support is provided by the NATO Computer Incident Response Capability Technical Centre in Mons, Belgium.[83] Moreover, NATO has also been developing Rapid Reaction Teams (RRT) that should be fully operational by the end of 2012. These cyber experts will be deployed within 24 hours to provide professional and well-organized technical advice to the member states and partner countries upon their request.[84] But the most important outcome from NATO's 2011 Cyber Defense Policy has been its proclamation to

maintain a strategic ambiguity toward Article V invocation in the case of cyber attack. In particular, NATO has agreed that a cyber attack can trigger a response under Article V, but the exact criteria for invoking the Article V would be left to the discretion of North Atlantic Council. According to the commander of the Allied Command Transformation, General Stephanie Abrial, every major incident will be analyzed separately and retaliated accordingly.[85]

Even though the speakers during a panel discussion on NATO's cyber defence in February 2012 sounded pessimistic on the short-term cyber future of NATO,[86] some progress has been made according to a staff member of the Estonian Defense Ministry. According to her, in October 2012 the status of the Practical Steps in the NATO 2011 Cyber Defense Policy could be described as follows:[87]

(1) Work has started on the development of minimum requirements for NATO relevant national information systems which is expected to be finished around 2014. However, according to the Estonian Defense Ministry, the heterogeneousness of cyber capabilities and infrastructure between the Allies have made this process tremendously challenging.

(2) Even though the priority of the Alliance is to assure the defence of its own networks or the basic cyber security, it has slowly started to turn its focus toward aiding the members in achieving the minimum level of cyber defense. In the Chicago Summit Guide, NATO stated that at this point NCIRC is prepared to assist Allies upon their request,[88] although its level of readiness is questionable until NATO has actually been able to demonstrate its effectiveness during a large-scale cyber attack.

(3) The 2012 NATO Crisis Management Exercise (CMX) is conducted concurrently with the 2012 NATO Cyber Coalition Exercise with the intent to test the functioning, effectiveness, and efficiency of collaborative cyber defense procedures and capabilities during a crisis situation.[89]

(4) The Alliance is working on integrating Cyber Defense into the NATO Defense Planning Process (NDPP)[90] to encourage increased investments into cyber-defense capabilities.

(5) Integration of cyber components into planning of operations is an important new task for the Allies that everyone takes quite seriously. In addition, the cyber components are already integrated into NATO's military exercises.

(6) NATO committees are currently drafting cyber policy toward its partners and the cyber defense requirements for its partners might be part of that.

(7) The strong authentication requirements are getting applied and NATO is working on streamlining the supply side.

(8) There have been no significant achievements in the enhancement of early warning, capabilities analysis, and situational awareness because the Allies are still struggling with trusting each other and sharing information. This aspect requires more collaborative efforts and sharing of lessons learned, and Estonia would like to see greater utilization of the CCDCoE in Tallinn by NATO for this purpose.

(9) Cyber components have been further integrated into NATO exercises, which should also help the Allies to focus on the awareness issues on strategic level.

(10) The list of sponsoring states of the CCDCoE has been expanding continuously. The US and Poland joined the center in November 2011 and the Netherlands in April 2012. Its cyber conferences have become increasingly more valued by cyber experts and the industry. Hence, the center has become a quite important nexus of the cyber debate and developments.

The Runaway Cyber-Train of Public Funds

Part of the reason for the creation of NATO was to assure the continuation of the democratic values that the Allies found imperative for the success of their societies. Under the Partnership for Peace program NATO emphasizes the importance of transparency, integrity and accountability in building defence institutions.[91] As Hari Bucur-Macru has said, "The real democratic exercise starts after the people have entrusted their representatives with the power to govern the society on their behalf,"[92] and this idea of transparency and accountability is even more vital to multilateral organizations that desire to maintain their integrity, including NATO. Unfortunately, the problems with large international organizations lie in the public oversight, as

they often lack transparency, especially in procurement. They are inward looking bureaucracies and are resistant to change because their organizational structures are ill-suited to new security threats. All these characteristics can be exacerbated in the defence institutions because the hierarchal restriction of information and situational awareness from public to secret. In the case of NATO there exists absolute lack of transparency about its budget and how it is used for the benefit of the Alliance's citizens.[93] The only aspect of the NATO budget that has been published is the cost-share arrangement.[94] Hence, the taxpayers have no other choice than to trust their representatives, who have been seconded by their governments or elected by ruling political parties, and the international staff with making reasonable decisions for the common good and assuring proper oversight of public funds.

Historically, but more than ever with the military operations in Iraq and Afghanistan, it has been observed that the oversight of domestic defence acquisitions and budgets is quite challenging and difficult.[95] Therefore, there should be made no illusions about the supervision of compliance in NATO, which has to assure accountability in the classified realm without impacting political consequences on staffs' careers and national policies. Hence, by allocating public money to the private sector, NATO has to assure accountability within a pool of people that is observably quite static on the international level; the same people changing the multilateral entities but not the level of influence in decision-making. The latter practice is one of the main corroders of the integrity of acquisition processes in the multilateral frameworks and makes NATO's ability to balance the tradeoffs between cost and effectiveness in the defence acquisitions questionable. This means that the Alliance should avoid huge procurement contracts on organizational level and leverage the risk management by promoting more collaborative efforts outside the official NATO framework, for example through Centers of Excellence, European Defense Agency, or multilateral agreements between the states. It is imperative for the success and future of NATO that it avoids positions that can erode public confidence and create doubt in its effectiveness among the Alliances' population, especially in the information society where the consequences of even small mistakes can become colossal to its existence.

On the other hand, the defence globalization has changed the conventional acquisition strategies. The contemporary defense procurement policies are extremely complicated and challenging endeavors. To be self-sufficient in the whole life-cycle (Development, Manufacturing /Production, Deployment, Operation, Training, Support, Verification, Disposal)[96] of product or system acquisition is no more feasible to most of the nation states because the extremely high costs and low scale of productions. Therefore, the procurement of defence systems is increasingly geared toward international cooperation and outright purchase, where the lowest cost-option would be the global consortia model that benefits from the division of labor and economies of scale.[97] Consequently, the Future Warfare will progressively incorporate a coalition doctrinal approach, [98] to which method the Allies under rising budget constraints cannot stay oblivious while repairing their capabilities' gaps and advancing their security because otherwise they would simply fall behind the possible adversary.

Hence, from the political point of view, any procurement recommendations made by NATO should be welcomed by public that expects its financial contributions to be utilized efficiently. Moreover, under a certain threshold (financial loss that would be acceptable to public) these acquisitions can and should be done by the Alliance to promote interoperability and cooperation. Meanwhile, from the civic point of view, the increasing contract amounts of NATO should raise great public concerns toward broader possibilities for corruption, insufficient oversight (auditing and monitoring), and inefficiencies in staff decisions.[99] Hence, the public-private partnership does not only advance the efficiency of services and products but also raises an ethical dilemma where profit-maximizing enterprises are facing the creator and maintainer of common good and benefits. Most importantly, it is not a responsibility of the private sector to produce valuable products and services for the society, but it is a duty of the institutions that award public funds to private sector to assure that the received products and services add value to the society. Currently, it is extremely debatable if NATO is capable of assuring the efficient utilization of public funds according to the contract specifications and expectations, especially in larger contracts that require more highly skilled, trained, and experienced staff, who besides

many other requirements should not be allowed to work in the defence industry after service in NATO at least for half a decade to avoid conflict of interest. Hence, ensuring compliance would be more than challenging if not almost impossible under current human resource structure of NATO.

Nevertheless, NATO has awarded two cyber related contracts, one directly and the other one indirectly relevant to the cyber domain. In May 2012 Northrop Grumman received a contract worth of €1.2 billion for NATO's Alliance Ground Surveillance (AGS) System,[100] from which Finmeccanica (Selex Galileo) received €140 million as a subcontractor.[101] AGS project should be considered as an indirect cyber-contract because without cyberspace the operation of Unmanned Aerial Vehicle (UAV) would be impossible from across the globe,[102] which also makes UAVs vulnerable to sabotage through cyber exploitation. For example, the Allies greatly underestimated the ingenuity of the adversary in Iraq and Afghanistan where the insurgents proved how easy it is to acquire strategic advantage because the relatively low cost of entry into the cyberspace and how challenging is the defense in cyberspace because the successful adversary needs to find only one vulnerable point of entry. Insurgents used $26 off-the-shelf software called SkyGrabber to hack into U.S. Predator drones and download video feeds because the communications' links of UAVs were not encrypted and thus left vulnerable for interception.[103] The U.S. Military personnel discovered laptops in Afghanistan and Iraq with hours of downloaded feeds from the drones, which suggest that counterinsurgency strategies of the Allies might have not always included the element of surprise. More surprisingly, some reports indicate that by 2012 only a fraction of the drones was encrypted, which means that the success of NATO's operations might have been jeopardized even after the Allies became aware of the vulnerability.[104]

On 8 March, 2012, NATO Consultation, Command and Control Agency (NC3A) awarded approximately 58 million Euros for cyber defense to Finmeccanica (SELEX Elsag and Vega) and Northrop Grumman Corporation. This project classifies as a direct cyber-contract because it should advance NATO Computer Incident Response Capability (NCIRC) from initial (IOC) to full

operational capability (FOC) that allows it to detect, assess, prevent, defend, and recover from cyber attacks against systems critically important to the Alliance.[105] According to NATO, the FOC should be implemented by the end of 2012 but the whole project is supposed to be finished in 12 months according to Brian Christiansen.[106] It should provide information assurance to around 50 NATO sites and headquarters throughout 28 countries.[107]This capability will be provided through highly software-intensive system that all C4I (command, control, communications computers, and intelligence) relevant contemporary systems qualify as in the defence acquisitions. Unfortunately, as the software becomes a more integral part of defense systems, the higher risk these systems entail because the software complexity, changeability, and invisibility, makes the monitoring of its development difficult.[108]

Meanwhile, in July 2012 Finmeccanica cyber solutions team reported that they had finished successfully the testing phase of the program's proof of concept,[109] which is just a second work package out of seventeen and means that there is still a long way to the product maturity and delivery.[110] For example, in the US DoD, software acquisitions are expected to follow systems engineering principles and according to the technology readiness level (TRL) the successful proof of concept is still equal to the infancy stage of the project.[111] In addition, there seems to exist an inconsistency about the value of the contract among all the interested parties. According to the RFP portion of the project there should exist a ceiling of €32,421,357 for the work packets 1 to 11 and 13,[112] but the contractors have stated for the award €50 million, NATO has reported for the awarded amount €58 million and the chief of NC3A cyber defence team, Brian Christiansen, has noted it to be €45 million. Hence, there appear to be at least three different amounts for the rest of the Work Packets, 12 and 14 to 17, if these values above the ceiling price indicate the cost of the rest of the contract and not the change in the ceiling price. Unfortunately without the transparent cost of the project it would be difficult to conclude why these discrepancies exist and how vulnerable they might make the project to become an easy target for "overheating." Problems that the British Ministry of Defence seems to be well acquainted with, as they complained about the inherited system procurements of the previous

office that according to them had frequently cost increases up to 40% between the point of acquisition and deployment.[113]

In any case, the future of NATO's cyber security is now in the hands of a company whose head of cyber solutions equates the NATO's contract with the Willy Wonka's Golden Ticket and believes that this contract will be catalyst for billions of dollars of public funds to the cyber industry.[114] Meaning, that the Defense Industrial Base that provides cyber security products is either acutely aware of the physics discipline or teachings of 19th century Prussian military strategist Carl von Clausewitz about the center of gravity. According to Clausewitz it is necessary to have effective intelligence capabilities and command mechanisms to overcome the challenges that arise from inherent difficulties and uncertainties of war - and what could possibly be more complex and uncertain domain for today's military strategists than a cyberspace. Clausewitz explained, "…. Out of these (adversary's dominant) characteristics, a certain center of gravity develops, the hub of all power and movement, on which everything depends. That is the point against which all our energies should be directed."[115] In the 21st century the cyber-based C4ISR[116] network (ICT network and the electromagnetic spectrum that allows the ICTs to function) is the source of power for network centric operations (NCO in US) or network enabled capabilities (NEC in UK, NATO), because the networks have the inherent capability to move payloads by themselves after the operators have entered the code or command into the interface.[117] Therefore, even though it is strategically essential for the Allies to assure full access to the global cyber commons, which has become with its networks a center of gravity for successful security strategy,[118] NATO also needs to bear in mind that the appropriation the taxpayers have entrusted to the Alliance for collective defense and security should be used prudently.[119]

Cyber Contract's Greatest Achievements

However, from the strategic and procurement point of view the most important part of the NCIRC contract is that the same contractors will be executing almost the entire life-cycle of the

defense acquisition by not only designing, testing and installing the cyber defense capability but also providing the subsequent maintenance and support for five years. Following a proper defense acquisition life-cycle has been one of the capabilities gaps for some of the European States. For example, in 2009 European Defense Agency concluded that the scarcity of deployable helicopters for European expeditionary missions was caused by inadequate maintenance and support of helicopters and insufficient training of their crews, and not by the actual amount of these airlift assets in European countries.[120]

Furthermore, it has to be emphasized that the NATO's NCIRC contract includes some extremely important clauses for assuring the security of the Alliances' digital infrastructure. The section 2.2 of the Invitation for Bid specifies that "no materials or items of equipment down to and including identifiable sub-assemblies shall be manufactured or assembled by a firm other than from and within a Participating Country."[121] The same applies to the labor side of the contract. This position might seem highly protectionist, but it is essential for guaranteeing a clean supply chain for the development of the NATO capabilities. The reason being, that not only administrative systems but also the weapon systems have become highly software dependent, which means that the attack surface of Allies has increased considerably and every effort has to be made to assure integrity from microchips to actual software program. For example, the aircraft's performance and capabilities have progressively shifted from being defined by physical hardware to being dependent of software. When in 1960 F-4 was 8% software dependent then by 2000 the fighter jets had evolved into open software-controlled aircraft systems,[122] as the F-22 is 80% software dependent and can be considered a cyber controlled aircraft.

Therefore, being oblivious of the supply chain would be even more dangerous to the Allies' and their digital infrastructure than any hacker per se. The Allies can develop the most advanced NEC and patch all the possible network vulnerabilities, but the security of Alliance would be still jeopardized if the communication or missile systems have defected or counterfeited microchips. In this case, the negligence of even one Ally, not to manage its defense supply chain properly, can compromise the operations of the whole NATO. Outsourcing manufacturing of equipment

parts or buying them from non-certified markets will only make Allies more vulnerable to hybrid threats, including cyber attacks. For example, procuring parts from China might be financially practical but definitely not the smartest defense approach. Everything that concerns the life-cycle of the defence system should be strictly confined to the countries that have no conflict of interest. It does not make much sense to spend valuable public resources on defending the Allied cyber domain against Chinese hackers stealing the Joint Strike Fighter designs and electronic data[123] if meanwhile Allies procure military-grade components for maintenance of defence systems, like F-15, from Chinese markets;[124]hence, willingly allowing its systems to be compromised. [125] This kind of negligent conduct for acquiring capabilities can definitely create strategies that categorize as "crapshoot" or "random walk."[126]

The military axiom that "generals always prepare to fight the last war instead of the next one" is considered a cliché but seems to be continuously relevant to our thinking about security, especially in the context of NATO. Being unprepared for the future is clearly an error of strategic importance that even Allies cannot avoid. Indeed, the fact that the Alliance is finally getting updated to the realities of the contemporary cyberspace by following through its 2011 Cyber Strategy does not prepare it for the future in cyberspace. As the Estonian president, Toomas Hendrik Ilves, emphasized at the 4th International Conference of Cyber Conflict, "In NATO, we will only reach the bare minimum acceptable level, defending NATO's own networks and N-CIRC FOC, in 2014. But NATO lacks a more ambitious vision for a post-2014 period."[127] Hence, to the organization that has to assure collective security to the transatlantic community, the cyber security does not entail solely the congruency with current cyber developments but also progression ahead of these developments and the ability to face the future challenges.

PART III - Ahead or Behind the Curve.

Armed or not Armed

"… [Temporary prohibition] was intended to fill what was perceived as a loophole at the time, but its promoters did not lose sight of the fact that it was an area that was developing exponentially. This rapid development subsequently hindered the ratification by the international community of a body of rules that would have imposed definitive restrictions on States."[128]

The above lines are not about the development of laws for the cyber domain but for one of its predecessors, the air domain. Ironically, also initial aeronautics designs were intended for peaceful purposes and flying was considered not of the slightest interest to the armed forces and therefore in early days air warfare was not subject to any specific legal regulations.[129] Hence, our society seems to suffer repeatedly from the Konrad Lorentz Paradox,[130] where the technological advances are created with peaceful intentions but end up causing destruction instead.[131] Therefore, it might be wise to start considering a precautionary principle[132] beyond justifying the environmental laws and the bias toward "adaptive error"[133] that explains pre-emptive strikes[134] and immense defense budgets.[135] Since the technologies and scientific endeavors constantly outpace the international and domestic laws and norms, our society persistently exists in a security vacuum where nobody is able to envisage or predict what the next armed attack or weapon will look like and once something different materializes it takes years before the obligations and compliance are updated and implemented. Therefore, instead of constantly amending and patching the treaties and regulations to reflect new means and methods, which is not a simple or inexpensive task for any government at domestic or international level, maybe these binding obligations should be rewritten to reflect consequences or to abolish narrow criteria.

The development of a consequence based normative framework for the emerging technologies to bridge the gap between kinetic and non-kinetic use of force and measures, is not a novel idea and was suggested already in 1999 by Michael N. Schmitt.[136] Consequently, this idea has been expanded more than a decade later by legal and technical experts in Rule 11 of "The Tallinn Manual on the International Law Applicable to Cyber Warfare" for defining the use of force in cyber space.[137] From one standpoint, "The Tallinn Manual" by NATO CCDCoE should be considered one of the most unique achievements with its attempt to clarify hostile conduct in cyber space; after all, achieving consensus on anything that concerns cyber operations has been quite rare. The Manual is a non-binding document that examines the aspects of cyber conflict in the context of *jus ad bellum* (regulating justification for armed conflict) and *jus in bello* (regulating conduct of armed conflict); for example, what constitutes a use of force and an armed attack and how to define sovereignty and jurisdiction in cyber space.[138] From another standpoint, it has taken our society, including the Allies, several decades to get to the point where a clarification of cyber conflict still requires 95 Rules over 186 pages, which demonstrates exactly the complexity of issues that technological advances have created for the Allies. Hence, this unofficial body of work might aid the governments, corporate entities, and international organizations in interpreting treaties and regulations for their code of conduct. However, its ability to make the Alliance more secure is questionable, because not everyone from kindergartener to adult reads and applies international law in their daily lives, but all of them do represent vulnerabilities in cyber security.

This general ambiguity in comprehension of all the facets of cyberspace is precisely why the adherence to Article 36 of Additional Protocol I of 1977 to the Geneva Convention[139] becomes even more challenging and complicated from "simpler" transparency issues that new military methods and weapons usually encompass. For example, this friction between modern warfare and oversight has become a noticeable political issue in the US during the last decade,[140] as well as in the case of US operations in Libya.[141] Modern wars are fought by utilizing Unmanned Arial Vehicles, Private Contractors, and Cyber Operations, but Remote War and Cyber War and their components were not imagined as means of warfare when the US War Powers Resolution was

written in 1973[142] and neither was this kind of evolution in warfare imagined by the drafters of the North Atlantic Treaty in 1949.

Furthermore, to accommodate the rights of governments for self-defense or *jus ad bellum*, our society has created double standards, laws for military and laws for civilians. It has always been extremely challenging to impose Geneva and Hague Conventions during conflicts - symmetric or asymmetric - because insufficient training and awareness of *jus in bello* and the lack of resources to enforce compliance and to comply to the International Humanitarian Law (IHL).[143] However, the application of these Conventions is even more challenging in the ambiguous cyber realm where it is currently almost impossible to apply the principle of distinction between civilian and military. Nevertheless, after decades of debate the consensus among most of the legal experts is that the "laws of war" in general apply to new technologies and scientific advances, including the cyber domain, although sufficiency of their clarity and application is contentious.[144] For example, the nation state can request its military to develop and launch a cyber attack, but the current attribution dilemma[145] in cyberspace would not allow the victim to determine if the attack was done by a civilian or the military. In addition, there exists a high possibility of the assault causing collateral damage, harming and affecting the civilian infrastructure, because most of the cyber infrastructure does not discriminate between civilian and military objects. NATO itself has admitted that in cyberspace commercial and military assets are highly inseparable while military operations are highly reliant on this infrastructure.[146]

In addition, *jus ad bellum* requires adherence to the principle of proportionality in utilization of countermeasures, but the cyber space offers a stealth capability that can have an escalatory effect in hostilities, because the responses to the attacks might be based on wrong assumptions caused by the attribution dilemma. The stealth capability and indiscriminate aspects of cyber operations has been well demonstrated by the Stuxnet worm. The fact that Stuxnet infected over 100,000 hosts and existed unnoticed for more than a year,[147] demonstrates the covert capability that cyber space can provide to all the belligerent actors, from private citizens to nation states. Moreover, according to the reports of Symantec Corporation, it was developed to

target exclusively Supervisory Control and Data Acquisition (SCADA) [148] systems and more specifically Programmable Logic Controllers (PLC) produced in Finland and Iran, even though Finland itself seems to have not been the intended target. In addition, the worm could copy itself from one removable media to another and thus also infect the non-network systems and spread without discrimination between military and civilian objects - from Indian satellite to industrial plants outside Iran.[149] Hence, Stuxnet that sabotaged Iran's centrifuges at Natanz Fuel Enrichment Plant in 2010 by changing the output frequency used for uranium enrichment[150] could be effectively considered a first generation cyber-weapon.[151]

Meanwhile, a valuable lesson should be learned from the recent developments concerning Stuxnet. In cyberspace it is axiomatic that the broader the knowledge or episteme of malware the more it will look like Medusa or a cluster bomb. As Lawrence Lessig noted in 1998 that in cyberspace "is an emerging sovereign that is omnipresent, omnipotent, gentle, efficient and growing."[152] As anticipated, the Stuxnet was really not a lonesome hunter but possessed a companion in Duqu that was discovered in 2011 and also seem to have cousins called Flame and Gauss, both discovered 2012.[153] According to cyber security analysts, all of these malwares are presumed to have been developed, employed, maintained by a nation state or sponsored by it because it requires significant resources that are not available to hacker groups or independent civilians. Furthermore, even though it has been impossible to establish the identity of the "anonymous belligerents" who are terrorizing the cyberspace with these targeted threats, the US and Israel have been considered as credible candidates by some analysts. At the same time, this information asymmetry between the attackers and defenders is the major reason why the targeted attacks are successful, while the reluctance to share forensic data and incident information hinder the development of effective and timely responses at a global level.[154]

Hence, it seems to be futile for Estonia and Visegrad Group to argue against militarization of cyberspace when cyber espionage is already in full swing; especially when one of the biggest members of NATO is treating cyberspace as any other operational domain[155] and very likely is developing and employing offensive cyber strategies. While in 2011 the US still argued that

developing robust cyber defenses no more militarizes cyberspace than having a navy militarizes the ocean,[156] one year later, in 2012, it emphasized that the US would respond to hostile acts in cyberspace as it would to any other threat to the country and it reserves the right to use all necessary means in cyberspace, although it will seek to exhaust all options before employing military force.[157] Moreover, the concerns over the militarization of cyberspace were emphasized at the 2012 International Conference on Cyber Conflict where the argument was made that "focusing on the strategic-military aspects of cyber security means subjecting it to the rules of an antagonistic zero-sum game" and invoking images of enemy even though one cannot definitely identify the enemy or obtain superiority in the cyberspace.[158] Unfortunately, looking at the recent history of cyberspace and the conduct of "anonymous belligerents," the shift in the perceptions in favor of cyber arms-race might have already happened and not just in some of the Allied countries, but also in other countries that can strongly influence the future of cyberspace, including Russia and China which are determined to keep up with the Allies.[159] Hence, at this stage it is becoming increasingly more challenging to balance between the possible consequences from preparing only for defense or for both (defense and offense), as the mistrust in the utilization of cyberspace is already prevalent. In fact, the spiral theorists argue that the psychological variables, like hostility and mistrust, can aggravate the misperceptions by contributing to the feedback cycle, which in turn will escalate the conflict.[160] Meanwhile, NATO is not only facing a growth of mistrust externally but also internally, as the Alliance itself is concentrating on the situational awareness and defense in cyberspace, while some Allies are also developing offense capabilities[161] and are contributing to the constant feedback cycle in the cyberspace.

Therefore, considering the above arguments about cyberspace - its indistinct comprehension, indiscriminate nature, and stealth capability – we should be concerned about the robustness of the North Atlantic Treaty. Cyberspace is an increasingly contested environment that is extremely dynamic and ever changing and thus the assumptions about its future or subsequent technological advancement being any different seem to be myopic. Hence, it is not surprising that the ability of the Treaty to accommodate the technological developments was questioned

in 2010 ACT Cyber Workshop where the proposal was made to "illuminate the current NATO's Treaty Article V wording to focus on the political interpretation more than the legal one."[162] The concern over the interpretation of attack in Article V was also emphasized in NATO's Multiple Futures Project one year earlier.[163] Ultimately it should be imperative for the Allies to assure that the Treaty will be strong enough to face the emerging challenges. Besides the controversy around the term "attack,"[164] the 1949 Treaty also contains the term "armed" that until now has caused relatively minor arguments among the Allies over cyber operations. Unfortunately, this kind of specification has the ability of becoming an inherent weakness of the Treaty in the future, or a "threat from within,"[165] unless NATO believes that all the subsequent inventions will be less ambiguous and will also accommodate decades' worth of debate over when and how an attack is "armed" before demonstrating devastating consequences to the Allies.

Maybe it is time to utilize Article XII of the Treaty[166] and review the adequacy of the Treaty in the light of the technological and scientific advances that already cause struggles in NATO today. "While international treaties can act as strategic instruments, they will be ineffective if nations do not clearly define treaty missions and objectives."[167] Hence, it might be a good time to start preparing the Treaty to face the 22nd century which unquestionably will include even more complex society and threats. Considering NATO's pace as concerns adjusting to new inventions, starting the review of the Treaty should be done as soon as possible to give the Allies sufficient time for debate and adaptations if necessary. After all, it took NATO eleven years - from the 1999 Kosovo conflict to January 2010 - to define in its glossary a term, such as "computer network attack" (CNA), which means "Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself" and noted that "a computer network attack is a type of cyber attack."[168] Add two more years for a preliminary definition of "cyber attack", which, according to the Tallinn Manual, is "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[169]

Inconspicuous Risks

During the last decade most of the Allies have been so caught up with finding solutions for hacking and cyber-crimes that some threats to the electronic infrastructure and systems have noticeably taken a back seat in their security analysis. Fortunately, NATO's strongest Allies - the US[170] and the UK[171] - have not been as oblivious to inconspicuous risks and have realized that being situated in the "Goldilock's Zone" of the solar system has not only encouraged the evolution of life and technological progress on earth, but also makes these advances vulnerable to the Sun's tumultuous cycles. Hence, monitoring and regulating cyberspace will not defend the Allies against strategic mistakes of not considering all other possible risk scenarios in the cyber domain. It is not only the virtual world and communications that require scrutinizing, but the vulnerabilities in the tangible electronic infrastructure itself. The more our lifestyle shifts toward electronics and digital equipment, the more leverage it requires against obscure and unexpected risks that are considered low-frequency high-impact threats, like a violent solar storm or Electro-Magnetic Pulse (EMP) incident. Although NATO has adamantly labored to prevent the proliferation of Weapons of Mass Destruction (WMD), including nuclear weapons that can cause an EMP, the likelihood of a nuclear (or weapon) EMP event is considered low by security analysts and it might never materialize. On the other hand, the likelihood of a severe geomagnetic storm or of violent space weather is much higher and, according to the scientists, the debates are not so much over if, but when, it will occur, and if it will coincide with the earth's overdue pole reversal, the latter potentially posing a worst case scenario. Therefore, monitoring of space weather should be as important as monitoring traffic on the internet.

Ultimately, nothing is immune to the space weather and we might be up for a bumpy ride as the solar activity is expected to approach its peak in 2013. The Sunspot Cycles wax and wane with an approximately 11-year cycle and expose the earth to changing magnetic disturbances caused by solar flares and coronal mass ejections. These events have caused considerable havoc in history, like the Carrington event of 1859 and the Quebec event in 1989, even if our society was then considerably less technology-dependent. Consequently, even though the Allies vary in

their electronic and digital posture, to mitigate geomagnetic risks all of them need more enhanced forecasting and monitoring capabilities, new GPS signals and codes, new-generation radiation-hardened electronics, and improved operational procedures.[172]

Even a more subtle danger than an EMP event would be the Allies' belief that providing objectives, ways, and means for the current cyber strategy would somehow permanently reduce the risks in cyberspace. Underestimating the three characteristics - complexity, adaptability, and rate of change - that distinguish cyberspace from other domains, would be the worst mistake any Ally could make, because NATO is as robust as its weakest link. It is imperative to comprehend that "today's cyberspace bears virtually no similarity to its predecessor of just two decades ago"[173] and its future will not be any less dynamic. The new software and devices that are perpetually incorporated into security systems make the systems more complex and make their managing ever more challenging. "The result is that while some means of cyber attack may be attenuated by these mechanisms, others may be introduced, and the overall attack surface may become larger and harder to understand. When systems with distinct mechanisms for implementing security policies are connected in new ways, inconsistencies may arise, introducing new gaps in the defense mechanisms that may be exploited by attackers."[174]

Therefore, NATO's view that the change in the internet protocol (IP) version, migration from IPv4 to IPv6[175], would somehow "decrease vulnerabilities or increase security in the cyberspace"[176] is extremely short-sighted and precarious. Beyond the necessary upgrade from a 32-bits to a 128-bits address that gives humanity 340 undecillion (10^{36}) IP addresses for the interfaces, the IPv6 seems not to diminish the security problems, including the attribution problem, but just shift them around or replace the old security problems with new ones,[177] inter alia malware tunneling that misuses this next generation internet protocol itself.[178] For example, in the case of attribution, a 2012 Guggenheim fellow, Susan Landau, has emphasized her concern over the personal-level identification at the packet layer as follows, "Although IPv6 has many more addresses than IPv4, it does 'not' contain any provision for identification of the

person using the machine. Therefore the attribution issue will remain the same after the transition to IPv6. By attempting to 'fix' the attribution problem by making Internet address level attributable to an individual is that such a solution would not solve the attribution in multi-jurisdiction multi-stage attacks, but would simultaneously have various negative consequences, including for law enforcement and national security."[179] In the case of more secure networks, Sean Convery and Darrin Miller have accentuated their concerns as follows, "in reality the same problems that plague IPv4 IP security deployment also affect IPv6 IP security deployment."[180] Moreover, the extensive transition period with inadequate support have made the security of the systems even worse, and in spite of promising characteristics of IPv6, the hackers have already demonstrated that it is not invulnerable.[181]

Hence, if the Allies are miscalculating the challenges of current IP migration which is just one component of internet, NATO's capability to face even more complex and sizeable future changes in the cyber domain is questionable. For example, adjusting to the vulnerabilities and advantages presented to the cyber security of NATO by migration of cyberspace to quantum era: utilization of quantum teleportation, quantum networks,[182] quantum computers,[183] quantum repeaters,[184] and transportation of enormous amounts of information extremely fast with photons and atoms.[185] Assuring cyber security and access to the cyber commons in the quantum era would be presumably more challenging and the increasing rate of technological advances suggests that its realization might happen before the turn of the century. For NATO to be ready for the quantum era, the discussions concerning the possible technological shift and its consequences should be commenced sooner rather than later, especially considering NATO's current slow tempo in keeping up with cyber issues.

According to Chip Elliot, Director of Global Environment for Network Innovations Project by National Science Foundation, the migration to quantum era does not only directly concern the future of cyber security but in the contemporary world extremely few people inquire about its consequences. For example, some of the following challenges are possible and should be already analyzed further:[186]

1) Creation of continental, and even inter-continental, systems for quantum teleportation will probably be within the realm of feasibility, as technologies are maturing quite rapidly.[187]

2) Early systems would likely be short-range, and at quite slow bit rates. Meanwhile, the physicists have already constructed a prototype for exchanging and storing quantum information. [188]

3) Quantum repeaters are the essential technology for making this all work at any practical distance.[189]

4) Quantum teleportation will allow the transport of arbitrary quantum information with some degree of fidelity. In particular, it can be used to send qubits between quantum computers, provide key material for quantum cryptography, and of course enable the teleportation of classical bits. The exchange of quantum encryption keys has been already done between an aircraft and ground station.[190]

5) Teleportation of classical bits would have a profound impact on cyber security, as the teleported bits do not "appear on the wire" anywhere between the transmitter and receiver. Thus it 'appears' to provide a very high level of information security, while we should not underestimate the creativity of people to find ways around it.

6) The overall architecture for a "teleportation-friendly" internet has not been thought out at all, but it is unlikely that the whole internet will be quickly converted to such technology. Thus, there would be special-purpose links at first, which might carry email messages. This means that the cyber domain might become quite fragmented as it shifts to quantum era, as the quantum internet might be analogous and complementary to the classical internet.[191]

7) Finally, the quantum teleportation might really not help with the authentication issue, so one will still need ways to authenticate the other end of a teleportation link.

Accordingly, concerns should arise if NATO is actually capable of comprehending the technological advances and adapting to their consequences. For example, the horizon scanning in the NATO's Multiple Futures (MF) Project does highlight the 'use of technology' as one of the deterministic drivers of change that will have a great impact on the future security of NATO but

the project does not give much attention to the possible structural change of the cyberspace or to technological shift.[192] Meanwhile the MF report demonstrates that NATO does recognize very well that technological advances cut both ways by increasing capabilities of the Alliance, as well of its adversaries.[193] Unfortunately, comprehending the dual-use of technologies and how the technologies can be utilized against NATO is not the same as apprehending how the technologies per se can cause vulnerabilities in NATO's capabilities or deficiencies in its abilities to defend the Allies. Hence, even though a rapid adaptability is a vital component of cyber security and mission resiliency,[194] NATO as an institution appears to lack this crucial characteristic for fulfilling its own intention to dominate in the cyber domain.

The Biggest Elephant in the Closet: The NATO Bureaucrat

Since "hierarchies have a difficult time fighting networks,"[195] "it is doubtful that traditional bureaucratic structures can keep pace with the rapidly evolving nature of cyberspace."[196] "Transforming current security organizations into network-based structures requires leaders who are comfortable with flexibility and dispersed authority"[197] and are acutely aware of the progress in the society. Hence, security organizations that are responsible for common security and defence, including NATO, need to tackle the biggest elephant in their closet – a human dimension and its turnover within its bureaucratic structure – if these organizations desire to be ahead of the security curve and not behind it. Accordingly, NATO's biggest impediment for comprehending the developments in cyberspace and keeping up with security challenges is its relatively static human resources and lack of real turnover.

The reason being, that the actions of the institution are greatly determined by those acting in the name of the organisation - its decision-makers.[198] Moreover, according to the international relations (IR) theory, decision-makers often draw analogies from history and from their own personal past experiences.[199] The behaviors and choices of the decision-makers are influenced by their cognitive capabilities, values, cultural perceptions, motivations, experiences, array of idiosyncrasies, and external factors. However, if the person never or rarely leaves the

multilateral bureaucratic environment, he or she would form analogies from extremely narrow range of events, his or her cultural perceptions and values would become distorted from reality, and his or her understanding of crucial characteristics of situations relevant to the current period would worsen and thus generalization and oversimplification would increase or become more prejudiced. Meanwhile scholars believe that any kind of generalization hinders rather than helps with productive thinking and that is why decision-makers fail to remove from the past events those facets that are ephemeral. As international relations theorist, Robert Jervis, explains this *post hoc ergo propter hoc* reasoning, "because the learning has not involved an understanding of many of the important causal relations, it is not general in the sense of grasping the crucial characteristics of the situation and the patterns that are likely to recur in the future."[200]

Regrettably to the organizations, the scholars also believe that the events can "exercise an especially powerful influence over an organization's memory if the organization's structure is altered so that part of it has a special interest in seeing that the previous event is taken as the model for the future."[201] The latter might be a reason why the multilateral bureaucratic systems progressively struggle to keep up with the accelerating developments in the 'info-bio-nano-robo-hydro-cogno' society. The personnel draw analogies from events that are persistently 'out of current context' because the organization is structured to promote the decision-makers who are homogenous in their perceptions and history; consequently, the model for the future will be 'stagnant' or 'lethargic adaption to surroundings'. These decision-makers would fail to comprehend properly the ever changing cyber domain and security risks that represent the actual external environment. Therefore, the more dynamic our society becomes because the increasing rate of technological changes, the superior adversary the static characteristic of the decision-makers will become for maintaining security, especially if the security organizations refuse to adapt to the continuously changing environment and to adjust their culture accordingly.

Nevertheless, NATO's comprehension about the necessity of diversity for creating competitive advantage[202] is extremely limited. The duration of rotation in NATO is three years after which the applicant can be extended for the post for another three years during which the position can be made indefinite; although maximum rotation for seconded staff is six years.[203] Such a prolonged service period, beyond 3 years, can impose cognitive deficiencies and biases in the decision-makers who according to the IR theorists are supposed to "operate in 'dual-aspect setting' where apparently unrelated internal and external factors become somehow related in the actions of the decision-makers"[204] or "play simultaneous 'two-level game' between domestic and international politics."[205] Hence, prolonged service in the multilateral bureaucratic system might seriously diminish or distort person's capability to play this 'two-level game' or operate in the 'dual-aspect setting' and lead to an increased tendency to "pay more attention to what has happened than to why it has happened."[206] In that case, it is not surprising that NATO as an institution lags behind its actual Allies in comprehension of security risks, especially in the tremendously volatile cyber commons – its staff is simply out of touch with continuous developments because it lacks more ample reciprocal influence and knowledge between domestic and international affairs.

For that reason, NATO's future employment efforts should be considerably more based on the premise that for the organization to survive and thrive there is an inherent value in diversity.[207] While the argument of Georges D'Hollander, General Manager of NATO C3 Agency (NC3A), that keeping up with technology has always been a challenge to NATO because the talent pool is being drawn to more lucrative areas,[208] might be actually a misguided conviction and consequently would permit NATO to ignore its inadequate human resource management and continue with 'business as usual.' Although it has to be noted here, that "NC3A consists primarily of NATO employed personnel in order to be independent of industry and national bias."[209] Additionally, the quality of staff might not be poor because it has not 'come up through ranks' or comprehend sufficient English,[210] but because the selection for positions, especially seconded posts, might be influenced more by political aspects than persons' actual capabilities to learn and adjust. Hence, the Alliance's hiring requirements might be emphasizing a wrong

skill set and background that do not provide NATO with necessary talent that is flexible, agile, adaptable, inquisitive, critical, and knowledge driven.

On the other hand, there are arguments among the Allies' military staff that the constant rotation has become detriment to achieving change because it is difficult to obtain commitments from ever changing community. [211] Nevertheless, military structures are learning how to embrace this dynamic process because it is essential for creating more agile and knowledgeable force that would be capable to think and act faster. To stay ahead of the adversary the evolution of C4ISR is based on developing next generation NEC/NCO, which requires a dynamic mindset.[212] Hence, currently it seems that the Allies' militaries are actually ahead of civilian counterparts in transforming themselves to a more dynamic entity, because civilian posts "can 'sit out' the changes initiated by military staff or appear to support the change but actually deliver very little."[213] Since NATO, similarly with National Defense Departments/Ministries, encompasses a military-civilian dual arrangement, the same problems are highly plausible within its structure. However, in the democratic system the military is not in charge of developing the policies and making the strategic decisions for society. Military's sole purpose is to be instrumental in the realization of the strategic goals, i.e. security and defense, if society is not capable of achieving them by diplomatic means. Therefore, in a democracy the elected political elite and the civilian staff possess the actual decision-making power and consequently should synchronize themselves with the evolution within the society, including the technological and scientific advances.

Accordingly, it is imperative for NATO to realize that in an 'info-bio-nano-robo-hydro-cogno' society it requires a more heterogeneous and dynamic human component within its structure and according to NATO's Multiple Futures Project it seems to recognize the necessity for more improved human intelligence that includes traditional and non-traditional groups of people.[214] Therefore, the strategy for tackling the human dimension should start from reassessing its policies that govern human resources.[215] For example, for NATO the turnover should be also horizontal across all the multilateral institutions, not just vertical within the entity. The current

trend where the same pool of people is just changing organizations, divisions and institutions, should be avoided. NATO needs to change its human resources policies to force its personnel to accept the dynamic environment. A person who has worked for a multilateral bureaucracy and made consecutively two rotations (like UN, EU, NATO, OECD, OSCE, etc) should not be allowed to apply for or be seconded to NATO positions. The person should prove in his or her application that after working for multilateral bureaucratic system, he/she has spent an equal time in a non-bureaucratic multilateral system, like the private sector, a think-tank, a NGO, a domestic institution, etc. Heterogeneous human resources are the best leverage against uncertainty that an organization can have, therefore it should not be surprising that bureaucracies with low turnover lack the capability to adapt to the dynamic world fast enough. One should not expect a person who is spending a decade or two within the multilateral 'bureaucratic bubble' to comprehend the complex challenges of the cyberspace that is extremely volatile and pervaded with uncertainty. While the increase in collaboration between industry, academia and institutions, will improve the comprehension of technological and scientific changes, it will not be enough to change the mindset of staffs that daily work within the same hierarchy, decision-making processes, conditions, and communicate with the same set of people. Decision-makers and staff actually need to change within the system, not just their positions and organization. It is imperative that these people step outside the 'bureaucratic bubble' and return to their community and have adequate amount of time to readjust to the scientific, technological, and social developments in the 'real world' before they reapply for a position that is responsible for the security of the whole transatlantic community.

Consequently, this would not just provide NATO with a competitive edge and sustain its robustness as an institution but it would also enhance its credibility in the transatlantic community and among the taxpayers who eventually are the ones who determine the success of the Alliance by agreeing to finance its expenses. NATO should not underestimate the power of public pressure in the ubiquitous information society and it should take its objective to 'win the battle of the narrative'[216] as a requisite for its survival and success. The observation: "Power

should not be left to speak for itself. It needs explaining if it is to be accepted,"[217] is not only relevant for resolving the conflict between 'a military at war' and 'a nation that is not'[218] or for countering an adversary's attempt to achieve a superior strategic communication, but this idea should be also applied for analyzing critically its own existence. Technological progress gives the transatlantic population increasingly more access to analyses and information about NATO, which will expand value judgments concerning the Alliance. Hence, NATO's success depends on the human dimension internally and externally. An internal threat arises from sequentially staffing its positions out of the same pool of citizens and consequently diminishing its capability to comprehend the risks, to adapt to the fast evolving society and therefore to protect the transatlantic community. The external threat arises from transatlantic residents who might decrease their positive assessments of NATO if they doubt its credibility and ultimately jeopardize its existence by allocating less public funds to the Alliance.

Conclusion

NATO's Global Commons Report seems to suggest that because the new Strategic Concept committed NATO to a strong defence posture in cyberspace, it would also somehow assure the Alliance to be at the front edge in assessing the security impact of emerging challenges. [219] This expectation might be attainable but definitely not while NATO suffers from a dichotomy between two contradictory perspectives. The Alliance as an institution appears to believe that it is as advanced as its strongest Ally, while the Allies separately seem to believe that NATO is as robust as its weakest link. Hence, for NATO to advance beyond its 'catching up' mode in the cyberspace, it has to critically analyze and acknowledge its current posture, because one cannot advance unless it accepts its vulnerabilities. As Charles R. Schwenk implies that under prior hypothesis bias, "decision-makers who believe that the institution's current strategy is successful may ignore information suggesting gaps between performance and expectations."[220]

Furthermore, it is imperative for NATO to realize that cyberspace is not just an increasingly contested domain but is also inherently contradictory. In cyber space everything thrives

reciprocally and the cliché 'what goes around comes around' is truly an accurate description of its character. Indeed, in cyberspace even good intentions can produce dreadful consequences when the code or interfaces have been modified from their original status. For instance, the net-centric architectures, like systems based on virtualization and cloud computing, do not only enhance operational effectiveness but also attack surface vulnerable for single point of failure where the payoffs for compromising the system are more generous.[221] That is why the U.S. Air Force Scientific Advisory Board emphasizes that the Allied military forces have to be capable to "fight through and continue to operate" in the presence of compromised systems.[222] Allies need to work on mission resiliency because none of them possesses capabilities to guarantee the resilience of the whole cyber infrastructure in the presence of persistent cyber attacks and counterattacks.

The cyberspace has permitted relatively simple systems to intertwine into extremely complex systems-of-systems. In the 'info-bio-nano-robo-hydro-cogno' society dissemination of intelligence between static and deployable components encompasses everything from satellite and ground-base communications systems, unmanned aerial vehicles, military platforms, awareness sensors, and weapon systems, to decision-makers. Network Enabled capabilities cover everything and everyone who contributes to the C4ISR Framework.[223] In the 21st century the relative advantage in the strategies of military and crisis management lies in the improved exploitation of knowledge that, in turn, depends heavily on information and communication technologies and virtualization. It is difficult to imagine efficient and effective NEC with a slogan of "Right information at the right place at the right time,"[224] without well managed cyberspace. However, "computer hacking is only limited by the attacker's imagination"[225] and the adversaries can limit the effectiveness of NEC by infiltrating the networks and sabotaging the information, by utilizing the Distributed Denial of Service attacks, by installing malware or a malicious code, etc. Hence today there is no political or military strategy without cyber dimension and the adversaries know how to exploit its vulnerabilities as well as the Allies.

Therefore, NATO's Treaty and defense strategy have to be capable of confronting an asymmetric warfare with hybrid threats that the existence of cyberspace has made readily obtainable. To win asymmetric war one requires enhanced intelligence that can be only achieved through better exploitation of knowledge and timely exploitation of new technologies, but unfortunately NATO as an institution currently lags behind most of its members in both. To enhance innovation and development of technologies NATO has to encourage progressive collaboration across Allies' defense industrial base. However, NATO will be able to support acquisitions and enhance its NEC only if it learns to utilize public funds efficiently, effectively, and transparently, because it needs taxpayers' support for developing and maintaining a strong posture on the global arena. Paradoxically, to become more robust, NATO requires more advanced and dynamic capabilities that are envisaged for the next generation NEC/NCO, but which the Allies cannot obtain and sustain without advanced cyber security. Consequently, for improved cyber security Allies have to promote superior digital awareness which can be only achieved through well developed strategies.

A robust strategy, including a cyber security strategy, is built on the idea that uncertainty is omnipresent and thus the future is unpredictable. All that Allies can do is minimize the risks and increase the probability for success by preparing alternative and back-up plans for the means and ways that have to lead to the acceptable ends. Even though the Estonian cyber incident might have helped the Alliance in realizing its past mistakes and how it was behind in cyberspace, it is now up to the Allies to find the willpower for changing NATO's outlook, including the cyber future. At the same time keeping in mind that they have to 'hang together' if they don't desire to 'hang separately' because none of them would be capable of facing the more complex and resource demanding next century alone.

ANNEX

Table 1. NATO Members Basic Information

Country	Capital	Population Total	Total Area (Km^2)	GDP 2011 (Current $US)
Albania	Tirana	3,215,988	28,748	12,959,563,902
Belgium	Brussels	11,008,000	30,528	511,533,333,333
Bulgaria	Sofia	7,476,000	110,879	53,514,098,360
Canada	Ottawa	34,482,779	9,984,670	1,736,050,505,051
Croatia	Zagreb	4,407,000	56,594	63,850,068,202
Czech Republic	Prague	10,546,000	78,867	215,215,310,734
Denmark	Copenhagen	5,574,000	43,094	332,677,281,192
Estonia	Tallinn	1,340,000	45,228	22,184,722,472
France	Paris	65,436,552	643,801	2,773,032,125,000
Germany	Berlin	81,726,000	357,022	3,570,555,555,556
Greece	Athens	11,304,000	131,957	298,733,589,250
Hungary	Budapest	9,971,000	93,028	140,029,344,474
Iceland	Reykjavík	319,000	103,000	14,059,073,613
Italy	Rome	60,770,000	301,340	2,194,750,339,253
Latvia	Riga	2,220,000	64,589	28,252,498,853
Lithuania	Vilnius	3,203,000	65,300	42,725,404,055
Luxembourg	Luxembourg City	517,000	2,586	59,474,583,333
Norway	Oslo	4,952,000	323,802	485,803,392,857
Poland	Warsaw	38,216,000	312,685	514,496,456,773
Portugal	Lisbon	10,637,000	92,090	237,522,083,333
Romania	Bucharest	21,390,000	238,391	179,793,512,340
Slovakia	Bratislava	5,440,000	49,035	95,994,147,901
Slovenia	Ljubljana	2,052,000	20,273	49,539,271,105
Spain	Madrid	46,235,000	505,370	1,490,809,722,222
The Netherlands	Amsterdam	16,696,000	41,543	836,256,944,444
Turkey	Ankara	73,639,596	783,562	773,091,360,340
United Kingdom	London	62,641,000	243,610	2,431,588,709,677
United States	Washington D.C.	311,591,917	9,826,675	15,094,000,000,000

Table compiled from World Bank Database 'WDI':GDP-Current US$ (Code: NY.GDP.MKTP.CD) Population Total (Code: SP.POP.TOTL) and Total Area from CIA The World Factbook: Country Comparison: Area.

Table 2. Technological Comparsion of NATO Members

	AL	BE	BG	CA	HR	CZ	DK	EE	FR	DE	GR	HU	IS	IT	LV	LT	LU	NO	PL	PT	RO	SK	SI	ES	NL	TR	GB	US
Index	27	10	28	5	20	18	1	12	11	8	24	19	7	21	17	13	9	2	3	22	14	26	25	15	16	23	6	4
A	27	10	25	2	23	19	1	12	11	9	24	16	8	26	18	17	6	3	4	21	13	28	22	15	14	20	5	7
1	26	12	28	6	23	16	2	11	8	7	25	15	10	24	19	17	1	3	4	21	13	27	22	18	14	20	5	9
1.01	14	17	27	4	20	26	2	10	6	8	19	13	11	25	24	22	1	7	3	16	18	28	23	21	15	9	5	12
1.02	25	14	22	10	24	17	2	1	11	13	26	18	7	23	21	15	3	5	4	27	9	28	20	12	16	19	6	8
1.03	26	10	27	4	25	20	1	9	12	3	22	16	8	14	18	21	7	2	5	13	15	24	28	19	17	23	6	11
1.04	13	12	24	4	25	21	2	11	9	7	22	17	8	27	19	16	5	3	1	18	26	23	28	20	15	14	6	10
1.05	15	12	24	5	27	20	3	10	8	6	25	23	9	26	18	14	1	2	4	17	22	21	28	19	13	16	7	11
1.06	25	10	27	8	23	19	2	12	3	7	17	16	9	20	22	24	1	4	6	21	14	26	18	13	15	28	5	11
1.07	28	3	27	7	20	10	4	19	11	5	24	13	17	17	23	20	1	7	9	20	12	26	14	16	15	25	5	1
1.08	24	1	24	20	23	4	17	17	8	9	24	17	4	28	4	9	1	1	16	22	11	11	13	13	24	20	7	13
1.09	7	15	21	23	20	24	11	14	5	8	25	9	12	27	6	1	4	17	2	26	19	16	22	28	18	13	10	3
2	28	8	20	1	24	22	2	15	14	13	23	19	6	27	16	17	10	5	4	21	11	26	25	9	12	18	7	3
2.01	25	5	27	8	20	16	6	14	7	12	22	17	2	24	23	15	11	3	1	26	9	28	19	18	13	21	4	10
2.02	28	6	14	5	26	22	8	9	10	11	25	27	16	23	12	24	2	4	1	19	17	18	15	21	13	20	7	3
2.03	10	25	3	4	6	23	2	26	27	20	19	24	5	28	9	17	1	12	14	16	15	18	22	7	11	13	8	20
2.04	3	1	22	3	12	25	7	12	12	20	17	1	3	7	21	26	24	16	12	28	3	19	22	7	27	7	18	7
2.05	8	3	4	1	14	25	4	8	8	25	27	4	8	14	4	14	14	14	8	14	8	14	14	2	27	14	14	14
2.06	28	1	26	9	27	7	17	11	5	4	24	15	22	20	23	21	16	3	12	14	19	25	13	18	10	6	2	8
2.07	26	10	23	19	24	18	5	15	21	n/a	1	17	6	12	11	4	27	14	7	9	16	13	22	3	8	25	20	2
2.08	19	1	25	3	23	22	9	14	4	13	26	20	7	12	18	17	16	6	11	21	10	24	27	15	5	28	2	8
2.09	15	10	16	9	27	17	4	6	12	8	25	21	3	26	20	22	1	5	11	23	7	24	28	18	19	14	13	2
B	26	10	27	2	16	22	5	12	13	8	21	23	1	17	14	11	9	6	4	19	18	20	28	15	24	25	7	3
3	28	10	18	2	22	12	9	11	14	8	20	27	1	21	23	17	7	5	3	19	16	24	26	13	15	25	6	4
3.01	28	6	16	3	25	9	12	8	5	10	17	23	1	19	27	21	14	11	2	22	20	24	18	7	13	26	15	4
3.02	25	6	4	16	1	11	n/a	4	16	16	6	16	16	16	24	1	6	26	27	16	16	6	10	15	11	1	11	11
3.03	26	6	13	16	19	12	4	24	11	9	22	28	1	14	23	18	8	2	7	21	3	17	27	10	15	25	5	20
3.04	28	10	26	8	20	12	3	11	14	9	24	21	1	22	19	17	6	2	4	16	18	27	23	13	15	25	7	5
3.05	28	6	23	8	21	13	4	7	19	12	25	11	1	27	20	9	10	3	5	26	14	24	18	16	17	22	2	15
4	21	22	27	8	6	26	5	19	23	13	16	20	1	10	4	2	11	15	7	17	14	12	28	24	25	18	9	3
4.01	21	25	27	16	7	19	1	18	23	4	22	14	3	6	5	10	9	17	2	15	11	24	28	12	26	20	13	8
4.02	11	6	17	8	12	28	19	20	13	25	4	23	7	10	3	2	22	18	24	16	21	1	26	27	14	15	9	5
4.03	26	24	28	1	1	21	17	1	1	1	24	18	1	27	22	16	1	1	1	22	1	1	20	1	1	1	19	1
5	23	1	27	2	17	19	5	7	6	8	22	15	3	21	18	11	12	4	14	16	24	20	26	10	25	28	9	13
5.01	13	2	26	3	22	14	5	12	10	6	28	20	1	21	17	16	11	4	8	18	19	23	27	15	25	24	7	9
5.02	12	1	25	2	9	21	10	7	5	16	20	11	4	23	17	8	15	3	24	19	27	14	22	6	28	26	13	18
5.03	27	5	26	12	21	24	3	9	4	10	13	15	7	14	23	16	17	1	6	19	8	22	25	18	2	28	11	20
5.04	26	7	22	7	21	7	7	1	7	7	25	6	7	20	2	3	7	7	7	5	27	24	7	4	23	28	7	7
C	25	11	27	8	21	17	1	12	10	6	26	18	9	20	19	15	7	3	2	23	13	28	22	16	14	24	5	4
6	27	12	26	9	18	20	2	11	10	7	24	22	5	13	23	14	3	6	1	21	17	25	19	15	16	28	4	8
6.01	6	18	8	28	3	7	11	12	25	10	21	14	22	1	24	2	4	16	15	13	5	17	20	23	19	27	9	26
6.02	25	11	24	8	21	16	5	12	9	7	26	18	1	22	14	20	4	3	2	19	23	27	10	15	17	28	6	13
6.03	28	9	27	7	21	19	5	14	10	6	24	17	1	18	20	23	4	2	3	15	22	25	12	13	16	26	8	11
6.04	28	10	27	8	22	17	5	13	9	6	24	17	1	21	19	16	3	2	4	15	23	25	14	12	20	26	7	11
6.05	28	9	22	10	21	23	2	12	5	7	17	18	4	15	19	16	6	1	3	25	20	24	26	13	14	27	8	11
6.06	n/a	21	27	6	14	26	3	7	10	16	25	19	17	12	13	18	11	22	1	5	8	20	23	15	9	24	4	2
6.07	15	10	20	4	25	14	2	8	11	16	27	26	1	17	21	12	9	6	5	28	13	24	18	22	19	23	3	7
7	24	10	28	11	25	13	1	12	8	2	27	20	6	18	19	16	9	3	4	23	15	26	21	14	17	22	7	5
7.01	20	10	28	12	21	15	3	13	9	4	23	19	1	26	24	17	8	6	2	25	11	27	18	22	16	14	7	5
7.02	28	7	25	11	22	12	4	15	3	1	27	18	10	13	19	20	8	5	9	21	17	24	26	14	16	23	6	2
7.03	28	8	26	11	20	17	1	15	6	2	21	16	9	13	18	22	7	3	4	25	19	27	23	12	14	24	10	5
7.04	26	12	20	7	21	11	4	1	10	13	28	23	3	25	18	5	14	9	8	19	16	27	15	17	24	22	2	6
7.05	11	6	28	9	27	13	1	14	12	8	25	24	10	26	16	17	3	4	2	15	18	19	22	20	23	21	7	5
8	18	12	23	3	22	21	4	6	7	11	26	17	14	28	20	15	9	8	5	24	10	27	25	19	13	16	2	1
8.01	15	14	24	9	21	22	5	3	11	8	23	18	10	27	20	16	1	12	7	26	2	28	25	17	19	13	4	6
8.02	13	14	19	12	25	22	3	4	9	11	28	17	8	24	21	15	1	10	7	26	2	27	23	20	18	16	6	5
8.03	27	9	18	2	15	14	8	12	6	10	24	11	20	28	16	13	23	7	5	21	21	16	25	19	4	25	3	1
D	26	10	23	6	20	17	2	7	9	8	27	18	11	21	19	12	13	1	5	25	16	28	24	15	14	22	4	3
9	27	10	25	8	23	18	2	9	7	5	26	20	11	16	19	13	12	1	4	22	17	28	21	14	15	24	6	3
9.01	19	14	24	7	25	18	9	3	2	11	27	22	6	21	23	12	13	8	4	26	10	28	20	17	15	16	1	5
9.02	28	9	26	7	21	17	4	11	6	3	20	16	14	13	23	24	10	1	5	22	18	27	19	12	15	25	8	2
9.03	16	12	23	7	22	21	4	5	9	11	28	26	8	25	19	10	13	6	3	24	14	27	20	18	15	17	2	1
9.04	n/a	5	23	7	22	10	3	14	9	8	19	16	2	13	11	12	n/a	1	4	20	24	26	18	15	21	25	6	17
10	24	8	22	4	19	18	2	1	10	12	27	17	15	26	21	11	16	5	7	23	13	28	25	14	9	20	3	6
10.01	26	9	23	12	22	18	2	3	7	10	25	20	1	21	19	14	4	6	5	28	8	24	27	17	15	16	11	13
10.02	24	8	20	6	19	9	4	2	23	18	27	15	1	28	16	14	10	3	7	21	13	25	17	12	22	26	5	11
10.03	17	16	22	10	27	19	4	1	7	14	23	20	3	21	24	12	6	8	5	26	2	28	25	18	15	13	9	11
10.04	25	10	16	4	14	25	6	5	8	7	19	15	28	21	17	11	24	8	13	20	17	23	27	12	1	21	2	3

Table compiled from World Economic Forum Insight Report.

Soumitra Dutta and Benat Bilbao-Osorio, "The Global Information Technology Report 2012: Living in a Hyperconnected World," Insead, World Economic Forum, Geneva: 2012.

For country codes see: ISO 3166-1-alpha-2 code. For corresponding text explanations for Column 1, see any Country Profile in the Global Information Technology Report 2012.

NOTES

[1] The author would like to thank Liina Areng, Dr. Susan Landau and Dr. Chip Elliot for their valuable contributions.

[2] According to the historian Jared Sparks, this was the reply of Benjamin Franklin to John Hancock's remark, the President of the Continental Congress, "We must all hang together" - at the official signing of the parchment copy of the Declaration of Independence on 2 Aug. 1776.

[3] John S. Duffield, "International Security Institutions-Rules, Tools, Schools, or Fools?: The Neorealist Baseline: Institutions (or Institutionalists) as Fools," in "The Oxford Handbook of Political Institutions," Oxford University Press, 2006, pp.639-642

[4] Richard K. Bretts, "Is Strategy an Illusion?" *International Security*, Vol. 25, No. 2, Fall 2000, pp.5-50.

[5] NATO, "The North Atlantic Treaty," 4 Apr. 1949, Washington DC., http://www.nato.int/nato-welcome/pdf/nato_treaty_en_light.pdf

[6] Derrick J. Neal and Linton Wells II, "Capability Development in Support of Comprehensive Approaches: Transforming International Civil-Military Interactions," CTNSP and INSS and NDU, Dec. 2011, pp. 65-86, http://www.ndu.edu/CTNSP/docUploaded/ITX2_Capability%20Development%20for%20CA.pdf

[7] Richard Higgott, "International Political Institutions: International Organization: Some Historical and Theoretical Insights," in "The Oxford Handbook of Political Institutions," Oxford University Press, 2006, p. 614.

[8] Michael W.Mosser, "Engineering Influence: The Subtle Power of Small States in the CSCE/OSCE," in Erich Reiter and Heinz Gärtner, "Small States and Alliances," Physica-Verlag, New York, 2001, pp. 63-84.

[9] Simon W.Duke, "Small States and European Security," in Erich Reiter and Heinz Gärtner, "Small States and Alliances," Physica-Verlag, New York, 2001, pp. 39-50.

[10] Erwin A. Schmidl, "Small States and International Operations," in in Erich Reiter and Heinz Gärtner, "Small States and Alliances," Physica-Verlag, New York, 2001, pp. 85-88.

[11] Guardtime, "Keyless Signatures: Technology Overview," 10 Oct. 2012, http://www.guardtime.com/ signatures /technology-overview/; In 2006, a team of Estonian cryptographers, network architects, software developers and security specialists got together to design and build a web-scale digital signature system for electronic data, using only hash function based cryptography. They named their invention Keyless Signature Infrastructure (KSI). The main innovations are the distributed delivery infrastructure designed for scale and the removal of the need to rely on cryptographic keys for signature verification.

[12] For comparison with NATO Members, please see Annex, Table "NATO Members Basic Information." Compiled Nov. 2012 from World Bank Database 'WDI': GDP: Current US$ (Code: NY.GDP.MKTP.CD), Population, Total (Code: SP.POP.TOTL) and CIA The World Factbook: Country Comparison: Area.

[13] World Economic Forum and INSEAD, "The Global Information Technology Report 2009–2010," Geneva, 25 Mar. 2010, http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf

[14] Trend Micro, "Operating Ghost Click, The Rove Digital Takedown," A Forward Looking Threat Research Team, 3 July 2012, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the_rove_ digital_takedown.pdf ; Federal Bureau of Investigation, "Operation Ghost Click," 9 Nov. 2011, http://www.fbi.gov/news/stories/2011/november/malware_110911

[15] Brigid Grauman, "Cyber-Security: The Vexed Question of Global Rules," A Security & Defence Agenda, McAfee and Geert Cami: Brussels, Feb. 2012, http://www.mcafee.com/us/resources/reports/rp-sda-cyber-security.pdf

[16] For a comparison with NATO Members, please see Annex, Table "Technological Comparison of NATO Members." Compiled Nov. 2012 from World Economic Forum and INSEAD, "The Global Information Technology Report 2012: Living in a Hyperconnected World," Geneva, 4 April 2012, http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

[17] Republic of Estonia, "e-Estonia," 1 Nov. 2012, http://valitsus.ee/en/government/e-estonia and http://e-estonia.com/ and http://e-estonia.com/components

[18] Patrick Kingsley, "How tiny Estonia stepped out of USSR's shadow to become an internet titan," *The Guardian*, 15 Apr. 2012, http://www.president.ee/en/media/interviews/7327-qhow-tiny-estonia-stepped-out-of-ussrs-shadow-to-become-an-internet-titanq-the-guardian/index.html ; Indrajit Basu, "Estonia Becomes E-stonia," *Government Technology,* 9 Apr. 2008, http://www.govtech.com/gt/284564?topic=117673

[19] Department of Homeland Security, "Cyber Storm: Exercise Report," 12 Sep. 2006, http://www.hlswatch.com/sitedocs/cyberstorm.pdf

[20] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine*, Issue 15.09, 21 Aug. 2007, http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=1

[21] Kadri Kask, Eneken Tikk, Liis Vihul, "International Cyber Incidents: Legal Considerations, "NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2010, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

[22] Häly Laasme, "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly*, Issue 63, 4th Quarter, 2011, National Defence University, http://www.ndu.edu/press/estonia.html

[23] Kenneth Geers, "Glance at the Mirror 2009: Cyber Defence," Estonian Foreign Ministry, 2010, http://www.vm.ee/?q=node/9071 and Kadri Kask, et al, "International Cyber Incidents: Legal Considerations."

[24] Determining the source, location, and identity of an attacker is an extremely challenging task. Fred Schreier, "On Cyberwarfare," DCAF Horizon 2015 Working Paper No. 7, pp. 34, 63-64, http://www.dcaf.ch/Publications/On-Cyberwarfare

[25]Alexander Klimburg, Heli Tirmaa-Klaar,"Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU," Policy Department, EXPO/B/SEDE/FWC/2009-01/LOT6/09, 15 Apr. 2011, http://www.europarl.europa.eu/committees/en/sede/studiesdownload.html?languageDocument=EN&file=41648

[26] Michael N. Schmitt, "The Tallinn Manual on the International Law Applicable to Cyber Warfare (Draft)," by International Group of Experts, NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE), Forthcoming in Cambridge University Press 2013, pp. 56, 68, 74,77, http://www.ccdcoe.org/249.html

[27] According to Article V, an armed attack against any Ally is considered an attack against all and Allies are expected to assist each other with necessary measures, including the use of armed force. NATO, "The North Atlantic Treaty," http://www.nato.int/nato-welcome/pdf/nato_treaty_en_light.pdf

[28] Ryan Kaiser, "Estonia: NATO's Cyber-Warrior," Central Europe Digest, 1 May 2008, http://www.cepa.org/ced/view.aspx?record_id=34&printview=1

[29] Larry K. McKee, "Cyberspace Senior Leader Perspective," CyberPro, National Security Cyberspace Institute, 30 Dec. 2010, http://www.nsci-va.org/SeniorLeaderPerspectives/2010-12-16-Eneken%20Tikk-NATO%20CCD%20COE.pdf ; CCDCoE, "28 October 2008," http://www.ccdcoe.org/21.html

[30] Estonian Defence League's Cyber Unit , http://uusweb.kaitseliit.ee/en/cyber-unit

[31] Tom Gjelten, "Volunteer Cyber Army Emerges in Estonia," NPR Interview with Estonian Defence Minister Jaak Aaviksoo, 4 Jan. 2011, http://www.npr.org/templates/transcript/transcript.php?storyId=132634099

[32] Susan W. Brenner and Leo L. Clark, "Conscripting and cyber conflict Legal Issues," 2011 3rd International Conference on Cyber Conflict, NATO Consultation, Command and Control Agency (NC3A), http://www.ccdcoe.org/publications/2011proceedings/ConscriptionAnd Cyber ConflictLeaglIssues-Brenner-Clarke.pdf

[33] Estonian Ministry of Defence, "Cyber Security Strategy 2008-2013," Estonia, Tallinn, 2008, http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

[34] For cyber strategies of other EU states see: ENISA, "National Cyber Security Strategies," May 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

[35] Christopher M. Schnaubelt, "Strategy and the Comprehensive Approach," Chapter 4 in Derrick J. Neal and Linton Wells II, "Capability Development in Support of Comprehensive Approaches: Transforming International Civil-Military Interactions," CTNSP and INSS and NDU, Dec. 2011, pp. 51-64, http://www.ndu.edu/CTNSP/ docUploaded/ITX2_Capability%20Development%20for%20CA.pdf

[36] Ibid.

[37] For more information about Visegrad Group see http://www.visegradgroup.eu/

[38] Joanna Świątkowska, Tomasz Szatkowski, et al, "V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations," The Kosciuszko Institute, 15 June 2012, http://v4cybersecurity.eu/

[39] Umit Kurt, "Cyber Security: A Road Map for Turkey," Strategy Research Project: International Fellow, Unites States Army War College, 2012, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA561300

[40] UK Cabinet Office, "UK Cyber Security Strategy: Protecting and Promoting the UK in Digital World," 25 Nov. 2011, http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf

[41] UK Ministry of Defence, "National Security Through Technology: Technology, Equipment, and Support for UK…" Feb. 2012, http://www.mod.uk/NR/rdonlyres/4EA96021-0B99-43C0-B65E-CDF3A9EEF2E9/0/cm8278.pdf

[42] Kim Sengupta, Jerome Taylor and Michael Savage, "Threat of Cyber Attack is the New Priority as Cuts Hit Major Project," *The Independent*, 19 Oct. 2010, http://www.independent.co.uk/news/uk/home-news/threatof-cyber-attack-is-the-new-priority-as-cuts-hit-major-projects-2110273.html; Eric Talbot Jensen, "President Obama and the Changing Cyber Paradigm," *Journal of the National Security Forum*, 31 Jan. 2011, *William Mitchell Law Review,* Vol. 37, No. 5049, 2011, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1740904

[43] IRL (Pro Patria and Res Publica Union) "Küberkaitse: Tunne Kelam: EL Vajab Terviklikku Küberjulgeoleku ja –Kaitse Strateegiat," 10 November 2012, http://www.irl.ee/tags/kuberkaitse; and Toomas Hendrik Ilves, "The President of Estonia at the International Conference of Cyber Conflict: Cyber-Security and Liberal Democracies," 8 June 2012, http://www.president.ee/en/official-duties/speeches/7589-the-president-of-estonia-at-the-international-conference-of-cyber-conflict-8-june-2012/

[44] Vincent Joubert, "Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO," NATO Defence College, Rome, May 2012, http://www.ndc.nato.int/download/downloads.php?icode=334;

[45] Rex B. Hughes, "NATO and Global Cyber Defense," Bucharest Conference Papers, German Marshall Fund of the US, 2008, pp.41-52, http://www.gmfus.org/bucharestconference/doc/08BucharestBook_web.pdf

[46] NATO, "NATO and Cyber Defence," 2 Aug. 2012, http://www.nato.int/cps/en/natolive/topics_78170.htm

[47] Atlantic Council, "NATO's Role in Cyber Security," Transcript, Federal News Service, Washington, 27 Feb. 2012, http://www.acus.org/event/transforming-towards-smarter-alliance-natos-role-cyber-security/transcript; and Spencer Ackerman, "NATO Doesn't Yet Know How to Protect Its Networks," 1 Feb. 2012, http://www.wired.com/dangerroom/2012/02/nato-cyber/#more-71379

[48] Stephen M. Walt, "The Origins of Alliances," Cornell University Press, 1987, pp. 1-49, 147-217.

[49] John Nagl, Richard Weitz, "Counterinsurgency and the Future of NATO," Transatlantic Paper Series No. 1, The Chicago Council on Global Affairs, Oct. 2010, http://www.thechicagocouncil.org/userfiles/file/task%20force%20reports/Trans-Atlantic_Papers_1_Nagl_Weitz.pdf ; "Smart Defense and the Future of NATO: Can the Alliance Meet the Challenges of the Twenty-First Century?" Conference Report and Expert Papers, The Chicago Council on Global Affairs, Mar. 2012, http://www.thechicagocouncil.org/userfiles/file/NATO/Conference_Report.pdf

[50] Nicola Butler, "Deep Divisions Over Iraq at NATO's Istanbul Summit," *Disarmament Diplomacy*, No. 78, July/Aug. 2004, http://www.acronym.org.uk/dd/dd78/78news01.htm ; and "Julianne Smith, "NATO: Allies in Action," *Defence News*, 19 July 2004, http://csis.org/press/csis-in-the-news/nato-allies-action

[51] Jason Healey, "Claiming the Lost Cyber Heritage," *Strategic Studies Quarterly*, Vol. 16, No.3, Fall 2012, Air University, pp.11-19, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf

[52] Clifford Stoll, "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage" Simon & Schuster Inc., 1989, http://mario.elinos.org.mx/docencia/herseg/cuckoo_egg.pdf; His personal account of tracking a computer hacker who had compromised the computer in Lawrence Berkley National Laboratory. (The 1982 Siberian Pipeline incident that supposedly was caused by the US written logic bomb, according to Thomas C. Reed, has been avoided here because the event has not been verified. Even the declassification of documents called "Farewell Dossier" in 1996 confirm this event beyond that US constantly fed defective technologies to Russia.)

[53] US Senate Permanent Subcommittee on Investigations, "Security in Cyberspace: The Case Study: Rome Laboratory, Griffiss Air Force Base, NY Intrusion," 5 June 1996, http://www.fas.org/irp/congress/1996_hr/ s960605b.htm ; and "Report of the Defense Board Task Force On Information Warfare-Defense," Washington, D. C., Nov. 1996, http://cryptome.org/iwd.htm

[54] Jason Healey, "Claiming the Lost Cyber Heritage," *Strategic Studies Quarterly*, Vol. 16, No.3, Fall 2012, Air University, pp.11-19, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf

[55] GlobalSecurity.org, "Eligible Receiver, " 5 July 2011, http://www.globalsecurity.org/military/ops/eligible-receiver.htm ; and Scott W. Beidleman, " Defining and Deterring Cyber War," Strategy Research Project, U.S. Army War College, 2009, https://www.hsdl.org/?view&did=28659

[56] Ibid.

[57] The White House "White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," , 22 May 1998, http://csrc.nist.gov/drivers/documents/paper598.pdf and The White House, "Protecting Cyber Security," National Archive and Records Administration, http://clinton5.nara.gov/WH/EOP/NSC/html/nsc-22.html

[58] Jack L. Brock, "ILoveYou Computer Virus Highlights Need for Improved Alert and Coordination Capabilities," US General Accounting Office , GAO/T-AIMD-00-181, 18 May 2000, http://www.gao.gov/archive/2000/ai00181t.pdf ; and McAfee, "A Good Decade for Cybercrime," 29 Dec. 2010, http://www.mcafee.com/us/resources/reports/rp-good-decade-for-cybercrime.pdf

[59] A zero-day attack is previously unseen attack on a previously unknown vulnerability. The adversary is aware of it but not the defender.

[60] Sadie Creese, Martin Sadler, Greg Williams, "Can Emerging Technologies Save the World: Securing Our Cyber Future," Oxford Martin School, Hilary Term Seminar Series, 22 Feb. 2012, http://www.oxfordmartin.ox.ac.uk/podcast/43

[61] Franklin D. Kramer, "Achieving International Cyber Stability," Atlantic Council, Sep. 2012, p.6, http://www.acus.org/files/publication_pdfs/403/kramer_cyber_final.pdf

[62] Kurt Hermann, "Connectivity is the Prerequisite for Successful Political and Military Engagement," *European Security and Defence*, 1/2010, http://www.europeansecurityanddefence.info/Ausgaben /2010/01_2010/ 05_Herrmann/Herrmann_01_2010.pdf

[63] If we consider 2012 deadline for the FOC. Brian Christiansen, "Cyber Defence Cooperation in NATO: How Did We Get to Where We Are?" NC3A, Apr. 2011, p.3, http://afdelingen.kiviniria.net/media-afdelingen/DOM100000140/Activiteiten_2011/KS2011_CYBER_OPERATIONS/Brian_Christiansen_-_NC3A.pdf

[64] The White House, "The National Strategy to Secure Cyberspace, " Feb. 2003, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

[65] NATO, "NATO and Cyber Defence," 2 Aug. 2012, http://www.nato.int/cps/en/natolive/topics_78170.htm? ; and Rex B. Hughes, "NATO and Cyber Defence: Mission Accomplished," *Atlantisch Perspectief,* Nr. 1/4, Feb. 2009, http://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf

[66] NATO, "NATO Opens New Center of Excellence on Cyber Defence," 14 May 2008, http://www.nato.int/docu/ update/2008/05-may/e0514a.html; CCDCOE does not belong to the NATO command structure. Its capital and administrative costs are covered by the host country, Estonia, while the rest of the expenses and the operating costs are shared by all the sponsoring states.

[67] There are five K's in the centers name in Estonian - Küberkaitse Kompetentsikeskus
[68] CCDCoE, "Past Events," http://ccdcoe.org/363.html
[69] CCDCoE, "NATO in the Cyber Commons ," 19 Oct. 2010, http://www.ccdcoe.org/199.html
[70] ACT Workshop Report, "NATO in the Cyber Commons," 19 Oct. 2010, CCDCoE, http://www.act.nato.int/images/stories/events/2010/gc/report05_tallinn.pdf; for another such view see Patrick Byrne, "NCSA-NATO's Lead in Cyber Defence," in "Connecting NATO: NCSA Under the Leadership of Lieutnant General Ulrich H.M.Wolf," Uwe Hartmann Edition, Hartmann Miles, Germany, 2009, pp.52-56
[71] Jason Healey, Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," Atlantic Council, Feb. 2012, http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf
[72] NATO, 'Smart Defence Smart TADIC," Background Paper, NATO, 14 Oct. 2011, p. 6. http://www.nato.int/nato_static /assets/pdf/pdf_topics/20120214_111014-smart_tadic_background.pdf ;
[73] NATO, "Centers of Excellence," 30 July 2012, http://www.nato.int/cps/en/natolive/topics_68372.htm
[74] Sean Lobo "NATO Transformation and Centers of Excellence: Analyzing Rationale and Roles," University of Oslo, May 2012, http://www.atlantic-community.org/app/webroot/files/articlepdf/CoEs.pdf
[75] NATO, "Exercising Together Against Cyber Attacks," NATO Multimedia, 20 Dec. 2011, http://www.natochannel.tv/?uri=channels/381662/1568212
[76] John W. Neptune, "Cyber-based C4ISR Assets: A U.S. Air Force Critical Vulnerability," Air University, Apr. 2009, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA539699&Location=U2&doc=GetTRDoc.pdf
[77] Luc Dandurand, "Rationale and Blueprint for a Cyber Red Team Within NATO," 2011 3rd International Conference on Cyber Conflict, NATO Consultation, Command and Control Agency (NC3A), 2011, http://www.ccdcoe.org/publications/2011proceedings/RationaleAndBlueprintForACyberRedTeamWithinNATO-Dandurand.pdf
[78] NATO, "Strategic Concept: NATO 2020: Assured Security; Dynamic Engagement," 17 May 2010, p. 12, http://www.nato.int/strategic-concept/expertsreport.pdf ; "*NATO must accelerate efforts to respond to the danger of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence.*"
[79] "Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats," 1500/CPPCAM/FCR/10-270038, NATO, Supreme Allied Commander (SAC) Europe and SAC Transformation, 25 Aug. 2010, p. 5, https://transnet.act.nato.int/WISE/CHTIPT/CHTKeydocu/BiSCinputf/file/_WFS/20100826_Bi-SC%20CHT%20Concept_Final.pdf
[80] Michael Aaronson, Sverre Diessen, Mary Beth Long, et al, "NATO Countering the Hybrid Threat," *Prism*, Vol. 2, No. 4, National Defence University, Sep. 2011, http://www.ndu.edu/press/nato-countering-hybrid-threat.html
[81] NATO,"Lisbon Summit Declaration,"20 Nov.2010, http://www.nato.int/cps/en/natolive/official_texts_68828.htm?mode=pressrelease
[82] NATO, "Defending the Networks: The NATO Policy on Cyber Defence," 8 June 2011, http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf
[83] "NATO and Cyber Defence," NATO A-Z, 16 Sep. 2011, http://www.nato.int/cps/en/natolive/topics_78170.htm
[84] "NATO Rapid Reaction Team to Fight Cyber Attack," NATO News, 13 Mar. 2012, http://www.nato.int/cps/en/SID-CE02A48A-209BF26A/natolive/news_85161.htm; and George I. Seffers, "Alliance to Deploy Cyber Rapid Reaction Team," 1 Sep. 2012, https://www.afcea.org/content/?q=node/10094
[85] Stéphane Abrial, "NATO Builds Its Cyberdefenses," The New York Times, 27 Feb. 2011, http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html
[86] Atlantic Council, "NATO's Role in Cyber Security," Transcript, Federal News Service, Washington, 27 Feb. 2012, http://www.acus.org/event/transforming-towards-smarter-alliance-natos-role-cyber-security/transcript
[87] E-mail was sent to the Estonian Defence Ministry for finding out the progress made in the Practical Steps of the NATO Policy on Cyber Defence. The 10 steps are listed in the end of the NATO Cyber Policy. Reply was received from Liina Areng in 8 Oct. 2012. This is not an exact translation of her reply, but interpretation.
[88]NATO, "NATO's 25th Summit Guide," 30 Aug. 2012, p. 104, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120905_SummitGuideChicago2012-eng.pdf
[89] NATO, "NATO Conducts Annual Crisis Management Exercise (CMX) and Cyber Coalition Exercise," 31 Oct. 2012, http://www.nato.int/cps/en/natolive/news_91115.htm?mode=pressrelease; "Estonia Participating in NATO Crisis Management Exercise CMX," *Estonian Review*, 1 Nov. 2012, http://www.vm.ee/?q=en/node/15778
[90] For information about NDPP see "NATO's 25th Summit Guide," 30 Aug. 2012, pp.72-84.
[91] Wim F. Van Eekelen, Philipp H. Fluri, "Defence Institution Building," Vienna, 2006, http://www.dcaf.ch/Publications/Defence-Institution-Building2
[92] Hari Bucur-Marcu, "Essentials of Defence Institution Building," Vienna and Geneva, 22 May 2009, p. 45, http://www.dcaf.ch/Publications/Essentials-of-Defence-Institution-Building

[93] Ian Davis, "Call for NATO Running Costs to Be Made Public on International Right to Know Day 10th Anniversary," 28 Sep. 2012, http://www.natowatch.org/node/769

[94] NATO, "Paying for NATO," 23 Apr. 2012, http://www.nato.int/cps/en/natolive/topics_67655.htm

[95]Commission on Wartime Contracting in Iraq and Afghanistan, "At What Cost? Contingency Contracting in Iraq and Afghanistan," Interim Report, June 2009, http://media.washingtonpost.com/wp-srv/politics/documents/ CWC_Interim_Report_06-10-09.pdf ; and the Final Report to Congress, "Transforming Wartime Contracting: Controlling costs, Reducing risks," Aug. 2011, http://www.wartimecontracting.gov/docs/CWC_FinalReport-lowres.pdf

[96] Department of Defense, "Systems Engineering Fundamentals," Defense Acquisition University Press, Jan. 2001, Virginia, pp. 7-8, http://ocw.mit.edu/courses/aeronautics-and-astronautics/16-885j-aircraft-systems-engineering-fall-2005/readings/sefguide_01_01.pdf

[97] Ron Matthews, "Smart Management of Smart Weapons," in "Studies in Defence Procurement," edited by Ugurhan G. Berkok, Queen's University, 2006, Canada, pp. 75-94, http://www.queensu.ca/dms/publications/ claxton/Claxton7.pdf

[98] Ibid.

[99] Todor Tagarev, "Chapter 7, Defence Procurement," in "Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices," NATO and Swiss Ministry of Defence, Geneva, 2010, pp. 72-85, http://www.dcaf.ch/Publications/Building-Integrity-and-Reducing-Corruption-in-Defence

[100] Northrop Grumman, "NATO Alliance Ground Surveillance," http://www.as.northropgrumman.com/ products/natoags/

[101] Finmeccanica, "Finmeccanica Wins a New Order Worth EUR 140 million….," 10 July 2012, Rome, http://www.finmeccanica.com/EN/Common/files/Corporate/Comunicati_stampa/2012/Luglio/ComFin_SELEXGalileo_NATO_10_07_12_ing.pdf

[102] Suzanne M. Vautrinot, "Sharing the Cyber Journey," *Strategic Studies Quarterly*, Vol. 16, No.3, Fall 2012, Air University, pp.71-87, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf

[103] Siobhan Gorman, Yochi J. Dreazen and August Cole, "Insurgents Hack U.S. Drones," *The Wall Street Journal*, 17 Dec. 2009, http://online.wsj.com/article/SB126102247889095011.html

[104] Shane McGlaun, "Report: Pentagon Fails to Encrypt Drone Transmissions," *TG Daily*, 31 Oct. 2012,http://www.tgdaily.com/security-brief/67192-report-pentagon-fails-to-encrypt-drone-transmissions

[105] NATO, "NATO Signs Contract for Cyber Defence," 8 Mar. 2012, http://www.nato.int/cps/en/natolive/ news_85034.htm ; NATO has removed the original page that was posted in 8 Mar. 2012 under NATO C3 Agency and included significantly more information about the contract.

[106] George Seffers, "NATO Set to Strengthen Cybersecurity," *Signal Magazine*, Aug.2011, https://www.afcea.org/content/?q=node/2686

[107] Finmeccanica, "Finmeccanica Cyber Solutions Team Awarded Contract to Provide NATO's Cyber Security Requirement," 29 Feb. 2012, http://www.finmeccanica.com/EN/Common/files/Corporate/ Comunicati_stampa/2012/Febbraio/FNM_NG__29_02_2012_ENG.pdf

[108] Defence Acquisition University, "ACQ 101 Fundamentals of Systems Acquisition Management : Lessons 21 and 22: Software Acquisition," 30 Aug. 2012.

[109] Northrop Grumman, "Finmeccanica Cyber Solutions Team Completes First Tests for NATO Cyber Security Programme Milestone," 11 July 2012, http://www.irconnect.com/noc/press/pages/news_releases.html?d=262046

[110] NATO C3 Agency, "Invitation For Bid to provide the NATO Computer Incident Response Capability -Full Operational Capability (NCIRC-FOC) IFB CO-13212-NCIRC," 20 Sep. 2011, p.15, http://www.defensa.gob.es/Galerias/info/servicios/concursos/2011/09/IFB-CO-13212-NCIRC-20Sep2011.pdf

[111] NASA, "NASA Systems Engineering Processes and Requirements w/Change 1," NPR.7123.1A, 4 Nov. 2009, pp.128-130, http://nodis3.gsfc.nasa.gov/npg_img/N_PR_7123_001A_/N_PR_7123_001A_.pdf; and graphical views at page 296 of "NASA Systems Engineering Handbook: Appendix G: Technological Assessment/Insertion," NASA/SP-2007-6105 Rev 1, http://www.acq.osd.mil/se/docs/NASA-SP-2007-6105-Rev-1-Final-31Dec2007.pdf

[112] NATO C3 Agency, "Invitation For Bid to provide the NATO Computer Incident Response Capability -Full Operational Capability (NCIRC-FOC) IFB CO-13212-NCIRC," 20 Sep. 2011, p.1, 32.

[113] Weber Shandwick, "Knowledgeshop: The Challenging Politics of Defence," Summer 2012, http://webershandwick.co.uk/media/doc/thinking_doc_1344423403.pdf

[114] Carlo Hoyos, "NATO to Begin Cyber Security Drive," 28 Feb. 2012, http://www.ft.com/cms/s/0/7afcaa96-6243-11e1-872e-00144feabdc0 .html#axzz2Byn3mh6o

[115] Carl Von Clausewitz, "On War" (Book Eight: War Plans) Edited and Translated by Michael Howard and Peter Paret, Indexed Edition, Princeton University Press 1984 (orig. 1976), pp. 595-596, 703; Gregory J. Rattary, "Strategic Warfare in Cyberspace," MIT, 2001, p. 80.

[116] Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.

[117] Dale C. Eikmeier, "Center of Gravity Analysis," *Military Review*, July-Aug. 2004, http://www.au.af.mil/au/awc/awcgate/milreview/eikmeier.pdf and "Redefining the Center of Gravity, *Joint Force Quarterly* (JFQ), Issue 59, 4th Quarter 2010, National Defence University (NDU), http://www.au.af.mil/au/awc/awcgate/jfq/eikmeier_redefine_ cog.pdf; Jan L. Rueschhoff and Jonathan P.

Dunne,"Center of Gravity from the Inside Out," *JFQ,* Issue 60, 1st Quarter 2011, NDU, http://www.au.af.mil/au/awc/awcgate/jfq/rueschhoff_dunne_cog_inside_out.pdf

[118] Mark Barrett, Dick Bedford, Elizabeth Skinner, Eva Vergles, "Assured Access to the Global Commons: Maritime, Air, Space, Cyber," USA, Virginia, 3 Apr. 2011, http://www.act.nato.int/images/stories/events/ 2010/gc/ aagc_finalre port.pdf

[119] Further discussion of counterarguments to the large scale NATO contracts is not in a scope of this paper and therefore it should be completed with few warnings: 1) From the governance point of view, the capability of NATO to funnel huge amounts of public money to private sector without transparent public oversight should be alarming for democratic systems. 2) From the economic point of view, NATO has to avoid the allocation of huge contracts to the same providers because this kind of conduct will become counterproductive to the promotion of the European and Transatlantic defence industrial base. If Allies are searching for economies of scale and competitive prices, they have to avoid promoting the concentration of the defence market. 3) From the governance point of view, the increasing influence of concentrated group of for-profit companies over the security of Allies should be a great concern and might produce a false sense of security. 4) For the success of NATO, it is imperative that a transparent tool would be developed for tracking the spending of Allies' contributions and how the Alliance guarantees the compliance.

[120] "European Defence Agency Special Bulletin: Helicopters – Key to Mobility," European Defence Agency, 10 Mar. 2009, http://www.eda.europa.eu/libraries/documents/eda_bulletin_11.sflb.ashx

[121] NATO C3 Agency, "Invitation For Bid to provide the NATO Computer Incident Response Capability -Full Operational Capability (NCIRC-FOC) IFB CO-13212-NCIRC," 20 Sep. 2011, p.20

[122] Lionel D. Alford, "Cyber Warfare: The Threat to Weapon Systems," *The WSTIAC Quarterly*, Vol. 9, Nr. 4, 2009, (Published 28 April 2010), http://wstiac.alionscience.com/pdf/WQV9N4.pdf

[123] S. Gorman, Y. Dreazen and A. Cole, "Insurgents Hack U.S. Drones," The Wall Street Journal, 21 Apr. 2009, http://online.wsj.com/article/SB124027491029837401.html

[124] B. Grow, Chi-Chu Tschang, et al., "Dangerous Fakes," BusinessWeek, 2. Oct. 2008, http://www.businessweek.com/magazine/content/08_41/b4103034193886.htm

[125] Sergei Skorobogatov, Christopher Woods, "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip," Draft, 5 May 2012, http://www.cl.cam.ac.uk/~sps32/Silicon_scan_draft.pdf; Richard K. Bretts, "Is Strategy an Illusion?" *International Security*, Vol. 25, No. 2, Fall 2000, pp.5-50.

[126] Richard K. Bretts, "Is Strategy an Illusion?" *International Security*, Vol. 25, No. 2, Fall 2000, pp.5-50

[127] Toomas H. Ilves, "The President of Estonia at the International Conference of Cyber Conflict," 8 June 2012, http://www.president.ee/en/official-duties/speeches/7589-the-president-of-estonia-at-the-international-conference-of-cyber-conflict-8-june-2012/

[128] Francisco Javier Guisández Gómez, "The Law of Air Warfare," International Review of the Red Cross, No. 323, 30 June 1998, http://www.icrc.org/eng/resources/documents/misc/57jpcl.htm

[129] Ibid.

[130] Robin Geiss, "Humanitarian Aspects of Cyber Warfare," in "International Humanitarian Law and New Weapon Technologies," International Institute of Humanitarian Law, 34th Round Table on Current Issues of IHL in 2011, 2012, http://www.iihl.org/iihl/Documents/IHL%20and%20new%20weapon%20technologies_Sanremo%20(2).pdf

[131] Konrad Lorenz, "Civilized Man's Eight Deadly Sins," R. Piper & Co. Verlag, 1973, English Tran., USA, 1974, p.12.

[132] "Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation." Principle 15 of 1992 Rio Declaration on Environment and Development, UNEP, http://www.unep.org/Documents.Multilingual/Default.asp?documentid=78&articleid=1163

[133] The fear of failure is why there seems to be a bias toward "adaptive error" (type II error) in IR as the penalties for wrong conclusions are extremely sever. Therefore the logic follows that it might be worse to miscast an expansionist power as status quo (type II error that leads to the failure of deterrence) than to incorrectly label the status quo power as expansionist (type I error that triggers a conflict spiral). For further information about the "adaptive error" in the work of James M.Goldgeier and Philip E. Tetlock, "Psychology and International Relations Theory, "*Annual Review of Political Science*, Vol. 4, June 2001, pp.67-92

[134] Marc Houben, "Better Safe Than Sorry: Applying the Precautionary Principle to Issues of International Security," CEPS, Working Document No. 196, Nov. 2003, http://aei.pitt.edu/1816/1/WD196.pdf

[135] Benjamin H. Friedman, "The Terrible Ifs," *Regulation*, Vol. 30, No. 4, Winter 2007-2008, http://www.cato.org/pubs/regulation/regv30n4/v30n4-1.pdf

[136] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law*, Vol. 37, June 1999, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993

[137] Michael N. Schmitt and International Group of Experts, "Tallinn Manual on the International Law Applicable to Cyber Warfare," NATO CCDCoE in Tallinn, Cambridge University Press, 2013, http://www.ccdcoe.org/249.html

[138] Ibid. Tallinn Manual: Rules 1-3, 10-14, 30; for a synopsis of Manual see Ashley S. Boyle, "Moving Towards Tallinn: Drafting the Shape of Cyber Warfare," American Security Project, Sep. 2012, http://americansecurityproject.org/featured-items/2012/fact-sheet-moving-towards-tallinn-drafting-the-shape-of-cyber-warfare/

[139] Parties are obligated to assess their military means before employment to determine if they are prohibited by international law. See ICRC, "Articles of Geneva Convention," http://www.icrc.org/ihl.nsf/WebList?ReadForm& id=470&t=art; for understanding acquisition point of view see Justin McClelland, "The Review of Weapons in According to Article 36 of Additional Protocol I," *International Review of the Red Cross*, Vol. 85, Nr. 850, June 2003, http://www.icrc.org/eng/assets/files/other/irrc_850_mcclelland.pdf

[140] Clay Wilson, "Network Centric Operations: Background and Oversight Issues for Congress," Congressional Research Service Report for Congress, 15 Mar. 2007, http://www.fas.org/sgp/crs/natsec/RL32411.pdf

[141] Julia Chen, "Restoring Constitutional Balance: Accommodating the Evolution of War," *Boston College Law Review*, 14 Aug. 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2129176

[142] In 1973 (as consequence of Vietnam War) the US Congress passed the War Powers Resolution (WPR) over President Nixon's veto to balance the powers and decisions of entering the war between executive and legislative branch. Therefore, President of the US has to seek Congressional Approval for sending US military to hostilities and only Congress can declare war. Today it is argued that legislative history shows that WPR is limited only to utilization of military personnel (boots on the ground). Hence, modern warfare technologies allow the president to act without Congressional Approval because the president is not sending the military personnel into hostilities. In the case of operations in Libya, when the Speaker of House warned the President that it was going to violate the time limits (60 days after notifying Congress within 48 hours of entering hostilities+ 30 days for withdrawal, if Congress don't authorize military action or declare war) allowed in WPR for American Forces to be involved in hostilities without Congressional Approval, White House replied that the level of American Forces in Libya was not considered as hostilities and therefore WPR did not apply. The operations did not involve sustained fighting or active exchanges of fire with hostile forces, nor they involved the presence of the US ground troops, US casualties or serious threat and therefore WPR did not apply.

[143] International Committee of the Red Cross, "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts," 31st International Conference, Geneva, Oct. 2011, http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf ;

[144]Wolff H. von Heinegg, "International Humanitarian Law and New Weapon Technologies," International Institute of Humanitarian Law, 34th Round Table on Current Issues of IHL in 2011, 2012, http://www.iihl.org/iihl/Documents/IHL%20and%20new%20weapon%20technologies_Sanremo%20(2).pdf

[145] US Air Force, "Cyberspace Operations: Anonymity and the Inherent Attribution Challenge, 15 July 2010, p.10, http://www.e-publishing.af.mil/shared/media/epubs/afdd3-12.pdf

[146] NATO Supreme Allied Command Transformation, "Managing Change: NATO's Partnerships and Deterrence in a Globalized World," Italy, 21-22 June, pp.III-7 to III-14, http://www.act.nato.int/images/stories/events/2011/ managing _change_hr.pdf

[147] Nicolas Falliere, Liam O. Murchu, Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response, Feb. 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_ dossier.pdf

[148] Acronym for Supervisory Control and Data Acquisition. For more information on their security risks see "Control System Cyber Vulnerabilities and Potential Mitigation of Risk for Utilities," White Paper, Juniper Networks, Inc., 2010, http://www.juniper.net/us/en/local/pdf/whitepapers/2000267-en.pdf

[149] James P. Farwell and Rafal Rohozniski, "Stuxnet and the Future of Cyber War," Survival: Global Politics and Strategy, Vol. 53, Nr. 1, 28 Jan. 2011, pp. 23-40, http://www.tandfonline.com/doi/pdf/10.1080/00396338. 2011.555586

[150] "IAnewsletter," *The Information Assurance Newsletter* by Information Assurance Technology Analysis Center (IATAC), Volume 14, Number 2, Spring 2011, http://iac.dtic.mil/iatac/download/Vol14_No2.pdf; Once Stuxnet entered the system it checked for the motor frequency range of 807 Hz and 1210 Hz, which is regulated by the Nuclear Regulatory Commission because it can be used for uranium enrichment, and changed the frequency to disrupt the long process of isotope separation. See James Grayson, "Stuxnet and Iran's Nuclear Program," Stanford University Physics 241, 7 Mar. 2011, http://large.stanford.edu/courses/2011/ph241/grayson2/

[151] Thomas Rid and Peter McBurney, "Cyber-Weapons," *The Rusi Journal*, Vol. 157, No. 1, 29 Feb. 2012, pp.6-13, http://www.tandfonline.com/doi/pdf/10.1080/03071847.2012.664354;

[152] Lawrence Lessig, "The Laws of Cyberspace," Draft 3, Mar. 1998, http://www.lessig.org/content/articles/ works/laws_cyberspace.pdf

[153] Boldizsár Bencsáth, Gábor Pék, et al," The Cousins of Stuxnet: Duqu, Flame, and Gauss," Special Issue of *Future Internet: Aftermath of Stuxnet*, Vol. 4, Nr. 4, Nov. 2012, pp.971-1003, http://www.mdpi.com/1999-5903/4/ 4/971; Kaspersky Lab, "Stuxnet, Duqu, Flame, Gauss: The High-End of Cyberwarfare," CERT-RO, 1 Nov. 2012, http://www.cert-ro.eu/files/doc/640_20121105151102024322900_X.pdf

[154] Ibid, Boldizsár Bencsáth, Gábor Pék, et al, p. 995.

[155] US Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, http://www.defense.gov/news/d20110714cyber.pdf; US Army, "Cyberspace Operations Concept Capability Plan 2016-2028," 22 Feb. 2010, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA516590&Location=U2&doc= GetTRDoc.pdf

[156] William J. Lynn, "Remarks on the Department of Defense Cyber Strategy," US Department of Defense, 14 July 2011, http://www.defense.gov/utility/printitem.aspx?print=http://www.defense.gov/speeches/speech.aspx? speechid=1593

[157]" Statement of General Keith B. Alexander Commander United States Cyber Command Before the Senate Committee on Armed Services," 27 Mar. 2012, p.7, http://www.armed-services.senate.gov/statemnt/2012/ 03%20March/Alexander%2003-27-12.pdf

[158] Myriam Dunn Cavelty, "The Militarisation of Cyberspace: Why Less May Be Better," 2012 4th International Conference on Cyber Conflict, NATO CCDCoE, Tallinn, June 2012, http://www.css.ethz.ch/publications/pdfs/ Militarization-Cyberspace.pdf

[159] How Russia combined cyber attacks with conventional warfare during Georgia-Russia 2008 conflict see Kadri Kask, Eneken Tikk, Liis Vihul, "International Cyber Incidents: Legal Considerations, "NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2010, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

For China's cyber capabilities see Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Northrop Grumman Corp., 9 Oct. 2009, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_ Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf; and 38th IFPA-Fletcher Conference on National Security Strategy and Policy, "Air, Space, & Cyberspace Power in the 21st Century," Jan. 2010, http://www.ifpa.org/pdf/USAFreportweb.pdf; Ian Easton and Mark A. Stokes, "China's Electronic Intelligence: Satellite Developments," Project 2049 Institute, 23 Feb. 2011, http://project2049.net/ documents/china_electronic_intelligence_elint_satellite_developments_easton_stokes.pdf

[160] Kenneth W.Terhune and Joseph M. Firestone, "Global War, Limited War and Peace: Hypotheses from Three Experimental Worlds," *International Studies Quarterly*, Vol. 14, No. 2, June 1970, p. 218.

[161] Jeff Kueter, "Cybersecurity: Challenging Questions with Incomplete Answers," *High Frontier,* The Journal for Space and Cyberspace Professionals*,* Vol. 6, No. 4, Aug. 2010, pp.29-30. http://www.afspc.af.mil/shared/ media/document/AFD-101019-079.pdf

[162] ACT Workshop Report, "NATO in the Cyber Commons," 19 Oct. 2010, CCDCoE in Tallinn, http://www.act.nato.int/images/stories/ events/2010/gc/report05_tallinn.pdf

[163] NATO, "Multiple Futures Project: Navigating Towards 2030," Final Report, Apr. 2009, p.33, http://www.iris-france.org/docs/pdf/up_ docs_bdd/20090511-112315.pdf ; and http://www.act.nato.int/subpages/nato-multiple-futures-project-documents

[164] Michael N. Schmitt, "Attack as a Term of Art in International Law: The Cyber Operations Context," 2012 4th International Conference on Cyber Conflict, NATO CCDCoE, Tallinn, June 2012, http://files.hash1.org/2012/10/ CyCon_book.pdf

[165] Phillip R. Cuccia, "Implications of a Changing NATO," Strategic Studies Institute, May 2010, pp.15-16, 38, http://www.strategicstudies institute.army.mil/pdffiles/pub990.pdf

[166] According to Article XII, the Allies can request for the review of the Treaty. NATO, "The North Atlantic Treaty," http://www.nato.int/ nato-welcome/pdf/nato_treaty_en_light.pdf

[167] Reyhaneh Noshiravani, "NATO and Cyber Security: Building on the Strategic Concept," Chatham House, London, 20 May 2011, p. 8, http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/ 200511nato.pdf

[168] NATO Standardization Agency, "NATO Glossary of Terms and Definitions," *Allied Administrative Publication,* AAP 6, 22 Mar. 2010, p.70, http://www.nato.int/docu/stanag/aap006/aap-6-2010.pdf;

[169] Michael N. Schmitt and International Group of Experts, "Tallinn Manual on the International Law Applicable to Cyber Warfare," NATO CCDCoE Tallinn, Cambridge University Press, 2013, p. 92, http://www.ccdcoe.org/249.html

[170] Kevin Cogan, "In the Dark: Military Planning for a Catastrophic Critical Infrastructure Event," CSL Study 2-11, US Army War College, May 2011, http://www.csl.army.mil/usacsl/publications/InTheDark.pdf; and After Action Report "Sever Space Weather Threats," National Defense University, 3 Oct. 2011, http://www.ndu.edu/inss/docUploaded/After%20Action% 20Report%20-%20Severe%20 Space%20Weather%20Threats.pdf; and for further reading in this subject see John Kappenman, "Geomagnetic Storms and Their Impacts on the US Power Grid," Metatech, Meta-R-391, Jan. 2010, http://www.ornl.gov/sci/ees/etsd/pes/pubs/ferc_Meta-R-319.pdf

[171]House of Commons Defence Committee, "Developing Threats: Electro-Magnetic Pulses (EMP)," Tenth Report of Session 2012-2012, UK, 8 Feb. 2012, http://www.publications.parliament.uk/pa/cm201012/cmselect/cmdfence/1552/1552.pdf

[172] "Severe Space Weather Events- Understanding Societal and Economic Impacts," Committee on the Societal and Economic Impacts of Severe Space Weather Events: A Workshop, National Research Council, National Academy of Science, 2008, http://www.nap.edu/catalo g.php?record_id=12507

[173] Matthew M. Hurley, "For and From Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance," *Air & Space Power Journal*, Vol. 26, No. 6, Nov.-Dec. 2012, pp.12-33, http://www.airpower.au.af.mil/digital/pdf/issues/2012/ASPJ-Nov-Dec-2012.pdf

[174] Rami R. Razouk and Frank C. Belz, "Meeting National Security Space Needs in the Contested Cyberspace Domain," *Crosslink Magazine*, Vol. 13, No. 1, Spring 2012, The Aerospace Corporation Magazine of Advances in Technology, http://www.aerospace.org/ publications/crosslink-magazine/spring-2012/

[175] US Department of Commerce, "Technical and Economic Assessment of Internet Protocol Version 6," Jan. 2006, http://www.ntia.doc.gov/files/ntia/ publications/ipv6final.pdf; and Jody R. Westby, Hening Wegner, William Barletta, "Rights and Responsibilities in Cyberspace: Balancing the Need for Security and Liberty," EastWest Institute and World Federation of Scientists, 2010, (Appendix A) pp. CSR43-CSR45, http://www.ewi.info/system/ files/Rights_and_Responsibilties_Web.pdf

[176] Mark Barrett, Dick Bedford, Elizabeth Skinner, Eva Vergles, "Assured Access to the Global Commons: Maritime, Air, Space, Cyber," USA, Virginia, 3 Apr. 2011, p. 40, http://www.act.nato.int/images/stories/events/2010/gc/aagc_finalre port.pdf

[177] INTECO-CERT, "Report on the Security Implications of Implementation IPv^6," June 2010, http://cert.inteco.es/extfrontinteco/img /File/intecocert/EstudiosInformes/cert_inf_security_implications_ipv6.pdf

[178] US-CERT, "Malware Tunneling in IPv6," 26 May 2005, http://www.us-cert.gov/reading_room/IPv6Malware-Tunneling.pdf; and Jeremy Duncan and US-CERT, "IPv6 is Here. Is Your Network Secure," 9 Aug. 2011, http://www.us-cert.gov/GFIRST/presentations/2011/ IPv6_is_Here.pdf

[179] Reply received from Dr. Susan Landau in 19 Oct. 2012. Attribution question was asked from her to clarify the conclusion of the following paper - David D. Clark and Susan Landau, "Untangling Attribution" in "Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy," National Academy of Sciences, Washington D.C., 2010, pp. 25-41, https://download.nap.edu/catalog.php?record_id=12997; or *National Security Journal* by Harvard Law School, 16 Mar. 2011, http://harvardnsj.org/wp-content/uploads/ 2011/03/Vol.-2_Clark-Landau_Final-Version.pdf

[180] Sean Convery and Darrin Miller, "IPV6 and IPV4 Threat Comparison and Best Practice Evaluation," CISCO, http://www.cisco.com/ web/about/security/security_services/ciag/documents/v6-v4-threats.pdf

[181] Ibid; and Kenneth Geers, "Strategic Cyber Security," NATO CCDCOE, June 2011, pp. 87-94, http://www.ccdcoe.org/publications/ books/Strategic_Cyber_Security_K_Geers.PDF

[182] Rodney van Meter, Kae Nemoto, et al, "Path Selection for Quantum Repeater Networks," *Networking Science,* 25 June 2012, http://arxiv.org/pdf/1206.5655.pdf and http://arxiv.org/abs/1206.5655; and Rodney van Meter, Joe Touch, et al, "Recursive Quantum Repeater Networks," *Progress in Informatics*, No. 8, 6 May 2011, pp. 65-79, http://www.isi.edu/touch/pubs/prog-in-informatics2011.pdf ; and http://www.nii.ac.jp/pi/n8/8_65.pdf

[183] N. Cody Jones, Rodney van Meter, et al, "Layered Architecture for Quantum Computing," *Physics Review X*, Vol. 2, Issue 3, July-Sep. 2012, http://prx.aps.org/pdf/PRX/v2/i3/e031007; and Rodney van Meter, Thaddeus D. Ladd, et al, "Distributed Quantum Computation Architecture Using Semiconductor Nanophotonics," *International Journal of Quantum Information*, Vol. 8, No. 01n02, Feb. 2010, pp.295-323, http://www.worldscientific.com/doi/abs/10.1142/S0219749910006435; or http://quantalk.org/articles/2009/07/09-07-001.pdf

[184] Peter van Loock, Thaddeus D. Ladd, et al, "Hybrid Quantum Repeater Using Coherent Light," *Physical Review Letters*, Vol. 96, Issue 24, American Physical Society, 19 June 2006, http://arxiv.org/pdf/quant-ph/0510202.pdf; Rodney van Meter, Thaddeus D. Ladd, et al, "System Design for a Long-Line Quantum Repeaters," *IEEE/ACM Transactions on Networking (TON)*, Vol.17, No. 3, p.1002-1013, 2009, http://arxiv.org/abs/0705.4128v2 and Quantum Physics, version 2, 7 May 2008, http://arxiv.org/pdf/0705.4128.pdf

[185] James Dacey, "Atoms Teleport Information Over Long Distance," *Physicsworld*, Institute of Physics, 22 Jan. 2009, http://physicsworld.com/cws/article/news/2009/jan/22/atoms-teleport-information-over-long-distance

[186]Reply received from Dr. Chip Elliot in 20 October 2012, also see, Chip Elliot,"Building the Quantum Network," *New Journal of Physics*, Vol.4, Issue 1, 12 July 2002, http://iopscience.iop.org/1367-2630/4/1/346/fulltext/ ; Please be aware that the author of this paper has added possible relevant information to the actual replies. Questions posed in the e-mail to Dr. Chip Elliot were the following: How is quantum teleportation valid to the future of cyber security. How would it change the current infrastructure that supports information exchange? Would we have to build a new infrastructure to support it? Since the current fiber optics cannot accommodate it because too much loss of information, is that is why there is research about quantum repeaters? It is supposed to allow more secure exchange of information between two interfaces. Would internet be still valid with quantum teleportation? How exactly quantum teleportation would fit into current cyberspace? Are we going to have two different levels of infrastructure, like e-mails and conversations might go through quantum teleportation, but internet will stay for all the general queries?

[187] Physics arXiv Blog, "Chinese Physicists Smash Distance Record for Teleportation," *MIT Technology Review*, 11 May 2012, http://www.technologyreview.com/view/427910/chinese-physicists-smash-distance-record-for-teleportation/; and "Europeans Physicists Smash Chinese Teleportation Record," *MIT Technology Review*, 21 May 2012, http://www.technologyreview.com/view/ 427969/european-physicists-smash-chinese-teleportation-record/

[188] John Matson, "First Universal Quantum Network Prototype Links Two Separate Labs," *Scientific American*, 12 Apr. 2012, http://www.scientificamerican.com/article.cfm?id=universal-quantum-network

[189] Stanford.edu, "Quantum Repeaters," https://www.stanford.edu/~sanaka/research/repeater.htm

[190] Sebastian Nauerth, Florian Moll, et al, "Air to Ground Quantum Key Distribution," QCrypt Conference, Singapore, 12 Sep. 2012, http://2012.qcrypt.net/docs/extended-abstracts/qcrypt2012_submission_12.pdf; and Jacob Aron, "Moving Plane Exchanges Quantum Keys with Earth," *NewScientist*, Issue 2882, 16 Sep. 2012., http://www.newscientist.com/article/mg21528824.300-moving-plane-exchanges-quantum-keys-with-earth.html

[191] Bassam Aoun and Mohamad Tarifi, "Quantum Networks," 19 Dec. 2003, pp. 61-63, http://arxiv.org/ftp/ quant-ph/papers/0401/ 0401076.pdf

[192] NATO, "Multiple Futures Project: Navigating Towards 2030," Final Report, Apr. 2009, p.33, http://www.iris-france.org/docs/pdf/up_ docs_bdd/20090511-112315.pdf

[193] Ibid, p.45.
[194] Elizabeth L. Scruggs, John Nilles, et al, "Meeting the Cyber Challenges of Tomorrow," *Crosslink Magazine*, Vol. 13, No. 1, Spring 2012, The Aerospace Corporation Magazine of Advances in Technology, 2012, http://www.aerospace.org/publications/crosslink-magazine/spring-2012/
[195] John Arquilla and David Ronfeldt, "The Advent of NetWar (Revisited)," in "Networks and Netwars: The Future of Terror, Crime, and Militancy," RAND Corporation, 2001, p. 15, http://www.rand.org/pubs/monograph_reports/ MR1382.html
[196] Jeffrey Caton, "What do Senior Leaders Need to Know About Cyberspace?" in "Crosscutting Issues in International Transformation: Interactions and Innovations among People, Organizations, Processes, and Technology," National Defense University, Dec. 2009, pp. 207-228, http://www.ndu.edu/CTNSP/ docUploaded /International%20Transformation.pdf
[197] Ibid, p. 217.
[198] For theoretical analysis of this supposition see R. Snyder, H.W. Bruck, B. Sapin, et al., "Foreign Policy Decision-Making (Revisited)," Palgrave MacMillan, New York, 2002.
[199] On drawing analogies see R. Snyder, H.W. Bruck, B. Sapin, et al., "Foreign Policy Decision-Making (Revisited)," Palgrave MacMillan, New York, 2002 , p. 158; and Robert Jervis, "Perception and Misperception in International Politics: Chapter 6: How Decision-Makers Learn from History" Princeton University Press, New Jersey, 1976, pp. 217-287.
[200] Ibid, Robert Jervis, "Perception and Misperception in International Politics, pp. 228-229.
[201] Robert Jervis, "Perception and Misperception in International Politics: Chapter 6: How Decision-Makers Learn from History: Organizational Learning," Princeton University Press, New Jersey, 1976, pp. 238-239.
[202] Taylor Jr. Cox, "Creating the Multicultural Organization: A Strategy for Capturing the Power of Diversity," Jossey-Bass, San Francisco, 2001, p. 141.
[203] For this information see the contract clauses in the notifications of the job vacancies at the NATO website.
[204] R. Snyder, H.W. Bruck, B. Sapin, et al., "Foreign Policy Decision-Making (Revisited)," Palgrave MacMillan, New York, 2002, pp.5,75
[205] Robert D. Putnam, "Diplomacy and Domestic Politics: The Logic of Two-Level Games," *International Organization*, Vol. 42, No. 3, Summer 1988, pp. 427-460, http://hpeb08.files.wordpress.com/ 2008/08/putnam.pdf
[206] Robert Jervis, "Perception and Misperception in International Politics: Chapter 6: How Decision-Makers Learn from History: The Learning Process," Princeton University Press, New Jersey, 1976, p. 228.
[207] Michàlle E. Mor Barak, "Managing Diversity: Toward a Globally Inclusive Workplace," 2nd Ed., SAGE Publications, 2011, pp.234-251.
[208] Georges D'Hollander, "C4ISR: A Comprehensive Approach," *Information & Security*, Vol. 27, 2011, pp.14-21, http://infosec.procon.bg/v27/27.02_Dhollander.pdf
[209] Frederic Jordan and Geir Hallingstad, "Towards Multi-National Capability Development in Cyber Defence," *Information & Security*, Vol. 27, 2011, pp. 81-89, http://infosec.procon.bg/v27/27.09_Jordan.pdf
[210] W.Bruce Weinrod and Charles L. Barry, "NATO Command Structure: Considerations for the Future," Center for Technology and National Security Policy, National Defense University (NDU), Washington DC., Sep. 2010, p.30.
[211] Derrick Neal and Louise Carver, "Delivering Network-Enabled Capability: The Importance of Innovation in Delivering Culture Change," in "Crosscutting Issues in International Transformation: Interactions and Innovations among People, Organizations, Processes, and Technology," NDU, 2009, pp. 55-74, http://www.ndu.edu/CTNSP/docUploaded/International%20Transformation.pdf; and Melanie Bernier and Joanne Treurniet, "Understanding Cyber Operations in Canadian Strategic Context: More Than C4ISR, More Than CNO," 2010 Conference on Cyber Conflict, CCDCoE, Tallinn, p. 236, http://www.ccdcoe.org/publications/2010proceedings/Benier%20-20Understanding%20Cyber%20Operations%20in%20a%20Canadian%20Strategic%20Context%20More%20than%20C4ISR,%20More%20than%20CNO.pdf
[212] Velizar Shalamanov, "NC3A As a Platform to Support C4ISR Capabilities Development for the Comprehensive Approach," *Information & Security*, Vol. 27, 2011, pp.47-64, http://infosec.procon.bg/v27/27.06_Shalamanov.pdf
[213] Derrick Neal and Louise Carver, "Delivering Network-Enabled Capability:..," National Defense University, Dec. 2009, p.61. http://www.ndu.edu/CTNSP/docUploaded/International%20Transformation.pdf
[214] NATO, "Multiple Futures Project: Navigating Towards 2030," Final Report, Apr. 2009, p.58,65, http://www.iris-france.org/docs/pdf/up_docs_bdd/20090511-112315.pdf
[215] Evangelina Holvino, Bernardo M. Ferdman, Deborah Merrill-Sands, "Creating and Sustaining Diversity and Inclusion in Organizations: Strategies and Approaches," Chapter 12 in "The Psychology and Management of Workplace Diversity," edited by Margaret Stockdale and Faye J. Crosby, Blackwell Publishing, 2004, pp. 245-276.
[216] NATO, "Multiple Futures Project: Navigating Towards 2030," Final Report, Apr. 2009, p.63, http://www.iris-france.org/docs/pdf/up_docs_bdd/20090511-112315.pdf; Joint Analysis and Lessons Learned Center (JALLC) , "The 2012 NATO Lessons Learned Conference Report," 31 Oct. 2012, Portugal, p.4, http://www.jallc.nato.int/newsmedia/docs/NLLC2012Report.pdf;

[217] Philip M. Taylor, "Strategic Communications and the Relationship between Governmental 'Information' Activities in the Post 9/11 World," *Journal of Information Warfare*, Vol. 5, Issue 3, Nov. 2006, p.11, http://ics-www.leeds.ac.uk/papers/pmt/exhibits/2831/JIW5_3_final_draft.pdf

[218] Mark C. Neate, "The Battle of the Narrative," United States Army Command and General Staff College, July 2010, p. 53, http://www.au.af.mil/au/awc/awcgate/sam/battle_of_narrative_neate.pdf

[219] Mark Barrett, Dick Bedford, Elizabeth Skinner, Eva Vergles, "Assured Access to the Global Commons: Maritime, Air, Space, Cyber," USA, Virginia, 3 Apr. 2011, p. 42, http://www.act.nato.int/images/stories/events/2010/gc/aagc_finalreport.pdf

[220] Charles R. Schwenk, "Cognitive Simplification Processes in Strategic Decision-making," *Strategic Management Journal*, Vol. 5, No. 2, Apr.-June, 1984, pp. 111-128, http://onlinelibrary.wiley.com/doi/10.1002/smj.v5:2/issuetoc

[221] Judith S. Kerner and Eltefaat Shokri, "Cybersecurity Challenges in a Net-centric World," *Crosslink Magazine*, Vol. 13, No. 1, Spring 2012, The Aerospace Corporation Magazine of Advances in Technology, 2012, http://www.aerospace.org/publications/crosslink-magazine/spring-2012/

[222] Rami R. Razouk and Frank C. Belz, "Meeting National Security Space Needs in the Contested Cyberspace Domain," *Crosslink Magazine*, Vol. 13, No. 1, Spring 2012, The Aerospace Corporation Magazine of Advances in Technology, 2012 , http://www.aerospace.org/publications/crosslink-magazine/spring-2012/meeting-national-security-space-needs-in-the-contested-cyberspace-domain/

[223] United Kingdom Ministry of Defence, "Understanding Network Enabled Capabilities," Newsdesk Communications Ltd., 2009, http://www.mod.uk/NR/rdonlyres/F40663B6-F2D2-4058-A1EB-B843559BCCB5/0/1926_NEC.pdf

[224] N. Ganuza, A. Hernández and D. Benavente, "An Introductory Study to Cyber Security in NEC," NECCS-1, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2011, p. 16, http://www.ccdcoe.org/articles/2011/An_Introductory_Study_to_Cyber_Security_in_NEC.pdf

[225] Kenneth Geers, "Strategic Cyber Security," NATO CCDCOE, June 2011, p. 23, http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF