US Foreign Policy Challenges: Cyber Terrorism & Critical Infrastructure

https://www.e-ir.info/2013/06/12/us-foreign-policy-challenges-of-non-state-actors-cyber-terrorism-against-critical-infrastructure/

NATALIA TERESHCHENKO, JUN 12 2013

US Foreign Policy Challenges of Non-State Actors' Cyber Terrorism Against Critical Infrastructure

Understanding why, how and with what consequences terrorists could and would want to use the cyber domain for their purposes is essential to formulating the best policy practices in preventing and managing the emergence of a cyber-empowered terrorist 'community'. Discourse analysis, epistemology and Sun Tzu's theory of war, along with other pertinent concepts of international relations provide a framework for looking at terrorists' motivations and activities in the cyber world.

Technological developments have seen the virtual domain evolve dramatically, and the 21st century marked acceleration in both- the online world and the threats that arise from it. The recent years have experiences not only an enhanced access to the internet worldwide, greater capabilities of programs and a wider range of services. Computers have also brought technical, political, social and economic problems, with malware being born at a higher frequency than the cures for it. Controls over targets and over attackers have become exceedingly difficult to achieve; and in the latter- practically impossible. More elaborate and complex hacking tendencies often target critical objects- private and public. Although for now, cyber is a domain of close attention in inter-state relations, the potential for terrorist groupings developing the capabilities, access and the motivation to target State and, indeed, private infrastructure is very serious. Many reports, research and intelligence information gathered suggest that in a couple of years from now, terrorists may acquire enough skills to use cyber space for attack purposes (Aitoro, 2009; GCN, 2012; Guneev, 2012).

The subject of cyber terrorism is situated within a very new field of research; therefore specific publications are very limited. However, positioned in a wider context, research easily overlaps with many disciplines, and these will be explored in detail. Authors, doctrines, governments and international organizations differ in opinion not only as to whether cyber terrorism is possible, but also as to the consequences of it, if taken as a plausible situation. I will provide a brief overview of the current prevailing lines of thought. Controversy in literature is largely based on the impossibility to define appropriately the terms and fit them into the existing legislation or into the policy of the state on cyberwarfare.

The FBI and CIA, NATO and the governments of US and other countries are hesitant about giving any specific information on cyber terrorism. In recent sources they tend to agree that it poses a high threat. Yet, whilst FBI may look like it is in fear on the scale and proximity of such an attack (Albanesius, 2012; Hoover, 2012), NATO may at the same time be saying that this threat has not yet emerged to a full scale. They both confirm, nevertheless, that it is only a matter of months or a year that terrorists may acquire sufficient expertise to perform an attack in cyber space (Brewster, 2012). All agencies, government officials- including even the former Deputy Chief of Bulgarian Intelligence (Focus News Agency, 2012) – and the technical sector, such as Kaspersky Labs or Symantec conclude that, as soon as terrorists get the sophistication, they will use it. In the very few years to come, says Eugene Kaspersky, we are likely to experience a cyber attack emanating from non-state actors and terrorists (Guneev, 2012).

What raises most discussions is the legality of response to cyber terrorism and how it fits into the law of war theory as

a whole, if that is at all applicable. Stewart Baker, the former Assistant Secretary for Policy under George W. Bush, believes that law puts unnecessary restrictions and acts as an impulse for disagreements on activities in cyberspace. When it is time to act to protect civilians and a nation, especially in offensive cyberwar, it may not be appropriate to look at the legality of the response. On the contrary, Charles Dunlap the former Deputy Judge Advocate General of the US Air Force, sees legal frameworks as indispensable and ethical- the absence of such may lead to war without limits (Baker; Dunlap, 2012). Dunlap also argues that it is not the absence of law *per se* that poses problems- it is the application of facts and complexities to the framework that renders judgements difficult (Dunlap, 2011).

Some, like Schmitt (1999) propose a new form of legislation, claiming that the existing one is insufficient to target the newly emerging threats. Prolific experts in the sphere, like Geers (2010a, 2010b) and Lewis (2010a), even suggest the adoption of a convention on arms control in cyberspace, which was discussed back in 2010, but never achieved a consensus (Homeland Security News Wire, 2010). Even internally, the recent attempt of the Congress to pass a new Cybersecurity Act has ended in a failure when the Republicans were reluctant to agree to the terms of the proposed Act, seeing it as governmental intrusion into businesses of private companies and into private lives overall (Levin, 2012; Vijayan 2012; Jaycox 2012). It seems when the threat is becoming greater, the reluctance of policy-makers to reach a compromise also increases.

Aristotle's Epistemology, the Discourse Theory and US Foreign Policy – Defining Cyber Terrorism in Theory and Practice

Embracing epistemology and the study of discourse, I found many analogizing principles that apply to the study of the cyber world and in particular, cyber terrorism. Aristotle's epistemology stems from the idea that true knowledge may only come from science, like the cyber domain. But even science- albeit in its purest form- cannot be the ultimate source of knowledge and cannot result in one system of such, as the predicates to it are so varied in content that they cannot be generic. The definition of objects and the development of understanding of these is the aim of knowledge, but every subsisting entity possesses Truth only to the extent to which it exists. In other words, the elementary cause of something is much more true and real than its posterior form (Aristotle, 2008). Applying this to cyber terrorism, we see that a universal definition may come only when we reach the elementary understanding of the being of the virtual world. But how possible is this when even this scientific domain is in development?

In parallel to Aristotle, the theory of discourse analysis looks at the content and construction of meaning, and how knowledge is organized according to social and political life (Crawford, 2004). Meanings are formed over time and within and across cultures, but, in contrary- or in addition- to Aristotle, they emanate from words and utterances. Discourses are implied in institutionalized power and are about political strength and distribution of such. A discourse functions as a structure; and both determines practices and is transformed by them. Articulation creates meaning through semiotic and linguistic connections between terms and meaning and by association, to institutions and social relations (Laffey, Weldes, 2004). Interpretation of the world representation evolves different identities, and, also in turn forms the functioning of the world. This theory echoes critical social constructivism in US foreign policy, where the world is said to be constituted through a series of meanings given by people and attached to things (Cox, Stokes, 2012).

Knowledge, therefore, may be seen as a socially constructed element, which differs in institutions, representations and realities, according to normative and ethical beliefs. An argument of interest states that political concern of critical actors formulates meanings (Crawford, 2004). This is what is exactly applicable to the cyber domain, where, according to current policies, countries admit and define threats. Socially, historically and nationally constructed, the connections on cyber terrorism are set in stone as a concept. But breaking articulations is possible – and will be attempted herein.

As a unit of analysis, we take the actual word 'cyber terrorism' and dismantle it into 'cyber' and 'terrorism'. If taken separately, or joined, we do not come to a satisfactory conclusion of the definition of the notion – it changes in the context, in its joint form with the other word and is different when stands alone. The discourse on terrorism is a bilateral and very polar system of signification. Both parties may even agree on the abstract definition of terrorism but as it has recently been seen at the counter-terrorist summit in Iran, the signifier of the discourse differs (Fars News

Agency, 2011). Our practice distinguishes from theirs, our motivations in our political discourse and definitions differ from their statutes.

Juxtaposing methods and policy practices in an attempt to deconstruct the truth may be a noble, yet meaningless undertaking, as, in the case of terrorism, what 'they' think will inevitably differ from what 'we' believe, as long as the policy practice remains on polar opposites. And it is at this point that we join science and language to determine what cyber terrorism actually stands for achieving a less modulated understanding of the discourse.

The terrorism discourse used by the US and indeed by any Western state sets the power relation and portrays terrorists as irrational, fanatic beings, creating the possibility of action. If, however, we would articulate them as militants that use power to challenge the US hegemony and obtain their political will- this would configure them as political opponents and thus make negotiation possible (Cox, Stokes, 2012).

In this context, Heidegger's differentiation between 'being' and 'existence' comes into play. Any object derives its meaning from a historically specific system of rules (Townshend, 2003). If we set those rules according to our beliefs, then we risk being misunderstood and political complications may result. If we, however, set our beliefs according to a set of rules, then we may succeed in creating a common understanding. I argue, therefore, that, in order to define cyber terrorism- and that will make it easier to address it- we have to unite the articulation and interpellation in a common denominator, facilitating thereby the construction of a multilaterally acceptable meaning. The fluidity of meaning calls for a transformation and viable articulation of, as far as possible, 'objective' discourse. To privilege understanding, we have to aim at capturing the essence.

In practice, cyber terrorism is a domain on which opinions diverge. Is it a separate phenomenon or just a facet of cybercrime, hacktivism or warfare? Should cyber terrorists be regarded as cyber criminals? The vast amount of literature written on security almost never differentiates between cybercrime and cyber terrorism. Some believe terrorists to be criminals and the methods and tools used seem to be identical in the cyber domain. However, cyber conflict is a complex notion that encompasses crime, security, terrorism and espionage (Carr, 2012; Tafoya, 2011). Terrorism is a form of politics, whilst cybercrime is more of a personal approach to technological attacks (Igantieff, 2004; Shackelford, 2009). A cyber attack is best understood not as an end in itself, but as an extraordinary means to accomplish almost any objective (Geerts 2011b).

I will reiterate that terrorism as such has to be seen as an attack on a much larger scale, affecting the lives, property and rights of a greater number of people than that caused by a crime. If stealing credit card information may be seen as a crime, the cutting off an electric power plant in Los Angeles is much more than a crime. Dunning summarizes it well: "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage" (Dunning, 2002). The intention also plays a role- if crime is usually committed for the financial benefit of the criminal; a terrorist attack usually has much more ideological, religious or political thought behind it, although financial gain may be a secondary incitement.

One of the potential definitions of cyber terrorism includes

"the use of computer network tools to shut down critical national infrastructures such as energy, transportation, government operations or to coerce or intimidate a government or civilian population" (Lewis, 2007).

There is another definition proposed by the FBI.

"A *criminal act* perpetrated by the use of computers and telecommunications capabilities, *resulting in* violence, destruction and/or disruption of services *to create fear by causing* confusion and uncertainty within a given population, *with the goal of* influencing a government or population to conform to a particular political, social, or ideological agenda"(Lourdeau, 2004, emphasis added).

To look from a very different point of view, Iranian General Massoud Jazzayeri believes that terrorism includes

"terror of thoughts and thinking, assassination of scientists, conventional assassination attempts, cyber terror, cutting city and transportation roads, and support for cultural discord" (Fars News Agency, 2012).

This paper understands cyber terrorism as an intentional act, performed through the use of information technology in an attempt to incite terror in the country, domain or population targeted, with the goal and/or effect of large-scale destruction, murder or infringement of rights.

Sun Tzu and the "Art of War"

Theories are inherently political by nature, and allow us to problematize concepts that exist. Much of the current military doctrine may be traced back to Sun Tzu, who's "Art of War" remains one of the classics for the conduct of armed operations. Whilst not easily transposed to the cyber domain, it has already been explored as a potential source for offensive and defensive deterrence tactics in this field, the challenges of which will be discussed later on in detail. It is essential to outline his philosophy of war and relate it to the strategy of the US in conducting warfare, especially virtually.

Sun Tzu was reliant on popular support and followed Confucius in his belief on war as being the last resort. The ideal war was one with no casualties- an attitude applicable to the first phase of cyber terrorism, when real-life destruction has not yet been caused (Handel, 1991). Sun Tzu's idea of operations puts emphasis on speed, surprise, economy of force, and asymmetry, and each of those indications being potentially the winning strategy in cyber warfare (Geers, 2011a). Some of advice given is aimed at making the enemy unprepared and confused- "caus[ing] division among them" and attacking the enemy's plans at their inception relates to the dismemberment of terrorist networks and applying defensive- or even offensive- deterrence (Sun Tzu, 2005; Handel, 1991). Direct confrontation and surprise cause victory of a battle (Sun Tzu, 2005). This principle should be applied to all retaliation and response mechanisms in virtual terrorism, where surprise is actually easy to achieve.

He calls upon intelligence gathering and deception, which is also crucial, albeit difficult, in the cyber domain. As it is a political activity, psychology in the preparations to war plays an important role in the whole domain of warfare. However, can we know our enemies in the cyber domain as Sun Tzu's postulates declare? Is there any decisive victory, to which Sun Tzu refers, but which we cannot grasp in the cyber domain?

As Geers states, Sun Tzu's theory is adaptable, though not sufficient, to encompass the world of cyberwarfare (Geers, 2011b). A useful tactic to apply for offensive and defensive deterrence schemes, Sun Tzu's approach does not, however, encompass prevention, law enforcement policies and other nuances that make the cyber domain such a difficult medium to handle and respond to.

Islamic Fundamentalism, the Religious and Ethical Dimension of Cyber Terrorism

Ethnocentrism, as a theory of international relations, may be applicable in the domain of cyber for the understanding of the motivations, ideology and actions behind cyber terrorist attacks and our response to them. We can explore the tensions between the Western and the Islamic- fundamentalist- thoughts. Centred in the ideas of one's own understanding of culture, religion, politics and society, the one civilization does not hold it necessary or important to understand the mentality of the other. It is focused on its own ethnicity and compares the values of the other in light of its own standards of culture. This theory may be set in parallel with the theory of American exceptionalism, developed as far back as Alexis de Tocqueville in the 19th century and continuing into the Bush administration (Provan, 2012).

The response to cyber terrorism may be squared into the same principles, if care is not taken. Sensitivity to the context and the understanding of meanings is, thus, of critical importance if there is to be effective international cooperation and policy making on all levels. In this context, the meaning of security is of primary importance- and how it differs from context, time, place and nation to another. The rhetoric of policy making in China is entirely different from that of the US. Whilst network security for the US encompasses human rights and the right to freedom of speech and expression, for the Chinese- security of the Internet is governed by national security, which overrides any potential human implications- in any case not recognized by the Chinese as crucial (Segal, 2012). On the other hand,

Russia would like to control what is accessed and available in the internet and sees as plausible to have access to private information; whereas for the US, this is not a solution (Giles, 2012; Markoff, Kramer, 2009).

With Islamic fundamentalism as a source of terrorism being a great preoccupation for the West, I will investigate the interpretation of the Quran in relation to cyberwarfare. Islamic scholars have issued many analyses, especially in relation to the use of force, sometimes even declaring fatwas. According to some recent media sources, the Islamic scholars have approved e-jihad and the use of the cyber domain for warfare (Geller, 2012). Al Suwaidan, one of the first Muslim preachers to openly propagandize Internet as means for jihad, has stated

"I strongly encourage young people to undertake electronic Jihad… I view this as better than 20 Jihad operations" (Stalinsky, 2012).

Fahd Bin Sa'd Al-Jahni, a Saudi lecturer in Islamic jurisprudence, also states that the Koran and the Sunna on jihad are applicable to cyber warfare (Stalinsky, 2012).

Jihad is a broad concept and may signify personal jihad, jihad by money and verbal jihad (Geller, 2012; Atayf, 2012, including citation from Sheikh Fahd Bin Saad Al Jahni). And although many scholars bring to attention that e-jihad may be harmful if used in the wrong circumstances or at the wrong time, they do not categorically prohibit or make explicit the fact that cyber terrorism is a wrong-doing. Jihad is not limited to military weapons, and, as long as the goal behind the attacks is being fulfilled, any means are allowed (Geller, 2012; Atayf, 2012, citing Dr. Mustafa Mourad). If referring directly to the Quran, we do not see a delimitation of weapons for violent jihad purposes- just the fact that Allah can limit the use of force. In addition, *49:015, Set 73, Count 149* states"…true believers …employ their substance and their persons in the defense of God's true religion…" (Natan). Although it may be said that e-jihad for now is limited to the preaching of Islamic ideas and spreading ideologies through the internet, or hacking Israeli sites; this does not exclude in any way the potential for a more diverse attack emanating from radical Islamic groups. Al Qaeda or the Taliban may be unable just yet to wage a full-scale cyberwar, but the actual fact that radical preachers approve of the use of the Internet should make us alert.

What are the advantages for non-state actors of using cyber as a medium for terrorist activities? There are a few, namely operational- attacks can be conducted remotely and anonymously- largely free of state support. This ensures that segmented networks are harder to penetrate and dismantle, and detection is difficult and takes time. Another advantage is the cost of such an operation and the ease of conduction on a variety of targets. For those who doubt how sensational the effect would be, it suffices to look at the chaos that is happening around the cyber domain, and stay 'reassured' that media coverage, in case of an attack, would be immense.

For some particularly zealous extremists, this would have a downside, as they will not die for their faith- something that can be done in suicide bombings, due to the low risk of personal injury in cyber attacks. Also, the achievement of a particular level of damage, emotional trauma and other desired effects may be limited and are highly dependent on precise configuration, expert technological control and other factors.

The Jus Ad Bellum and Jus In Bello in the Just War Theory

According to the 'western moral tradition', the defense of threatened values is the only justifying cause for war. These values include the protection of the innocent, the punishment of the evil and defense against a wrongful attack in progress (Johnson, 1992). And Johnson does not see the moral tradition as easily allowing for a defensive strategy. According to the moral tradition, we would equate ourselves to terrorists, if we were responding in a 'supreme emergency' manner (Johnson, 1992).

The just war subjects our actions to a legitimate authority and just cause, along with the right intention. To be just, the war has to comply with the jus ad bellum and jus in bello. Proportionality, necessity, discrimination and sovereignty are key principles (Carr, 2012). Jus ad bellum, jus in bello and jus post bellum consider the different stages of an attack and may be applicable to any attack, including in cyberspace.

When we come to a satisfactory definition of cyber terrorism, and, as long as the attacker is to wage war- or what he believes to be war, he is respondent to the law of armed conflict. Of course, there exists the debate as to whether terrorists have the right to wage war, or are respondent to the above Conventions, which were destined to the state-to-state relations. Our perception of terrorists is that of an illegitimate group, which obeys no laws. Therefore, it may be said that they are also not subject to any laws, including the bellum iustum. Holding these individuals as morally accountable may also prove difficult, as this raises the never-ending debate of morality, ethnocentrism and east-west tensions.

However, interestingly enough, the Penal Code of the Islamic Republic of Iran, in its article 183 stipulates that whoever resorts to arms to wage terror and panic shall be considered an 'enemy combatant'- this contradicts to a recurrent analysis and interpretation of the Geneva and Hague Conventions' (Islamic Republic of Iran, 1991; UN, 2005). Yet, arguably, terrorists may be lawfully attributed the status of 'enemy combatants' when both parties see themselves at war. This will increase their responsibility in front of international law, but will also protect inviolable human rights in judicial pursuit.

Challenges and Advice for Policy Makers

Legal Measures and Policy Aspects

The current lively debate is whether policy makers and the military should develop a strategic and operational field in cyberspace, or whether lawmakers should set guidelines and restrictions in the first place. The pertinent arguments for both sides include the fact that legal questions that arise in the cyber world limit the planning or potential conduction of cyberwar by the military. At the same time, cyberwar without legal bases would create chaos an illegitimacy- lawyers are so deeply embedded into the national strategic and intelligence sectors that without them operations are critically undermined (Brust, 2012). I will argue that one does not exclude the other and parallel measures should be taken, in order to prevent possible future attacks, at the same time limiting the effect of potential attacks that may take place in the nearest future. Establishing international cyber norms should be set as a priority.

At this point, it is essential to remember that one of the highest challenges in strategy is the balance of interest and values. Upholding values, like freedom of speech and the right to information, and, at the same time, addressing broader national interests and even the protection of these same values obscures our policies (Davis, Jenkins, 2002; Fars News Agency, 2012; Inquisitr, 2012). It is in finding the right momentum between what is crucial in individual life, and what is fundamental for the nation- and indeed, for these very own individuals, who, if faced with a cyber attack lose not only their rights, but, perhaps, lives- is a decisive and critical point. That is why, for the moment, there are discussions and debates, and yet no concrete actions plan in the cyber domain (Westby, 2012).

International legislation is a difficult stance. A challenge faced by lawyers is whether they should insist upon compliance with the existing law of war restrictions in conducting any counter-attacks, cyber warfare or deterrence moves. Or should fear of the unknown dimensions of cyberwar lead us to abandoning the concept of the law of war and drive us out of the limits for preventive, pre-emptive or safety purposes (Brust, 2012)?

Russia sees cyber weapons as comparable to WMD and aims at banning it with an appropriate treaty, whereas the US sees the need for more international cooperation for criminal prosecution (Carr, 2012). In 2009, Russia proposed to develop a cyber-arms control treaty on the model of the Chemical Weapons Convention of 1997. The fact that Russia and the US were talking with a UN arms committee shows a policy shift and desire to somehow join forces in addressing the now-burning issue. However, due to the specificities of cyberspace, prohibition and inspection are two main challenges which prevented the two countries from agreeing on law enforcement issues (Geers, 2010b; Markoff, Karmer, 2009). The rationale of the US in maintaining space dominance and the belief that it is premature to address cyber terrorism in a legal capacity should be left in the past, and movements in this direction are already being made. The White House reiterates the need for compromise and legislation (White House, 2011).

Of course, there emerges a cyber arms race concern. The US is rapidly developing its capacities and cyber weapons, and training staff in the cyber domain. Russia, on its own side has always been strong in individual

capacities of technically skilled personnel. China's strengths are increasing in the sphere, whilst North Korea is by now a cyber danger for States. Yet, it is the responsibility of States to address the issue of cyber weapons as it has been done with nuclear weapons. A pertinent level of protection and a well-rounded legislative framework will prevent threats and attacks emerging not only from States but also from non-state actors and make it easier to address the hazards, should there be any arising. The most sensitive issue is the states' capabilities of a successful malware attack. Whilst terrorists may pose a threat as non-state actors, states can be no more immune to a cyber law, if such were to be ratified. They would also have to be subject to it, meaning that covert operations- if we presume that Stuxnet and Flame were developed by nation states- would be forbidden. This may not suit some major powers and thus become a limit into the ratification of such a law, as the political will could change dynamics.

The question whether the US will also be willing to use cyberspace as a domain to conduct its own strategic military operations may affect the policy it may have to adopt towards the terrorist or extremist groups using it so. Politics includes not only physical power, but also legitimacy, and this has to be remembered by the US policy makers when devising a strategy for cyberspace. Inter-agency mechanisms should be established to create coherent unified policy guidance with roles, responsibilities and application of activities determined across the whole sector. This reflects the "unity of command" principle of war.

Although it is extremely hard to ban the use of cyber weapons in general, due to the fact that it is hard to define a cyber weapon, and that most instruments may be harmless; it is possible to outline a regulatory effects-based framework. Combining a zero-sum game of arms control and a non-zero sum game of developing the law and conventions is an optimal balance. The US should be pro-active in encouraging international arms control for cyber arms by, firstly, modifying its own cyber crime legislation to be in tune with international agreements and trends. The next step would be in creating new regulations for the private sector, software and hardware companies, and domestic infrastructure (Wilson, 2006). Mutual disarmament and deligitimization of cyber weapons is a complicated process, for which the society may not seem ready at the moment. Technically, it is problematical, as cyber arsenals emerge and develop at a speed higher than it is possible to classify them. There should be an action consensus and policy between states on the elimination of the first-use of viruses, worms and similar 'arms'. A monitoring system of parallel security issues- such as in the spheres of missile and nuclear defence, conventional arms and maritime security, should be established, thus making it easier to monitor the complicated cyber space.

There also exists a possibility to delineate the Internet and cyberspace as a source of free information and equate it to "national heritage" or similar status, thus legalizing the protection of any intrusion or covert operations. International legal instruments governing space, high sea and, for example, the Antarctic, do not allow for nationalization. The same policy may be applied to cyberspace. Certain authors, like Johan Eriksson and Giampiero Giocomello adopt a neoliberal constructivist approach, stating that it is essential to view the internet as a world with its own customs; therefore, states must come together to create a common understanding, thus ensuring the development of the internet and sustainable security of it.

Broadening international law enforcement coordination, specifically through the Europe Convention on Cyber Crime is a good starting point as territorial jurisdiction is less likely to be an effective deterrent in a borderless world. It is evident that such a framework cannot answer all questions, for example that of attribution of the attack. Drafting an international regime on the basis of the above and other existing conventions and protections in the spheres of maritime, space, and communications laws could do justice in creating a legal baseline for cyber terrorism and cyber space protection. Creating a legal standard for the time of peace and the time of cyberwar would enable to consolidate the international humanitarian law with the newly developed instruments (Shackelford, 2009).

A burning question is how to incorporate law enforcement and empower prosecution, at the same time increasing court capacity? A very complex question would lie in the judgment of cyber terrorist cases and training of law enforcement officials and criminal officers.

An effects-based approach would also seem the most pertinent. When an attack leads to genocide or causes massive killings, it may be judged according to prevailing standards. Compliance and enforcement should be monitored- this will also minimize the chances of state-sponsored terrorism. A good choice would be to set up an

independent authority or agency for oversight and control. This agency could also be responsible for *ex ante* surveillance, detection and interdiction of intrusions into critical infrastructure and other online systems

Policy dimensions of cyberwar include the possibility to deter others from resorting to it (Libicki, 2009). Policy makers facing the assessment and targeting of future cyber threats should address key issues from multiple perspectives. Preparedness and prevention is one aspect: information sharing and establishment of good practices, along with public-private partnership is of a primary importance. Detection of and response to threats via an alert system would dramatically increase the timely targeting of attacks. Contingency plans and disaster recovery would mitigate the attacks. International cooperation and the establishment of active defenses for critical infrastructure should also be in place (Carr, 2012).

An extremely vital, yet unbelievably complex sphere, the bounding of cyber terrorism into a legal framework requires a long-term engagement by the international community. Conceivably, Internet service providers could be ordered by law to cut off services to users whose machines demonstrate an unusual pattern of outgoing packets. Yet many threats would still remain- DDoS cannot corrupt or crash systems, and does not affect traffic internal to server-restricted spaces, so how can it be regulated? And how would regulations, law enforcement and judgements differ if the attack would emanate from a State or from a non-state actor? (Libicki, 2009).

Socio-Political Awareness and Cooperation

The mobilization and sustainability of political will is critical. As top-down, so bottom-up approaches to leadership in the sphere of security have to be constructed. A broad, deep and inter-disciplinary knowledge and specialization of the field has to be established and shared. Influence of the media and strong advocacy towards policy-makers will ensure a comprehensive understanding and tackling of the issues. A realist plan of action with details and targets has to be set and structural processes- as institutional, so organizational- will prove beneficial in advancing the strategic practice and implementation of policies (Evans, Kawaguchi, 2009).

Politically unsafe recommendations may often harm the global approach to fighting cyber terrorism. However, standing still in the situation is a wrong move. Full disclosure is the best policy in a potential response to a cyber terrorist attack (Libicki, 2009). The internal and international political, social and economic consequences of a cyber attack have to be taken into account when formulating a policy.

Short-term goals should be set elaborating on the benchmarks to be achieved in the next 5 years. Long term action agenda should also be established. This should include the creation of cooperative political conditions nationally and internationally to be able to achieve consensus on what is now seen as divergent opinions. Transparency of States should be achieved. For this, increasing the technical capacity and cooperation of countries is vital. Military conditions should also be balanced, so that the cyber domain is no longer seen as a means for waging offensive or defensive operations- instead it should be set as a stabilizing unit of space. verification and monitoring conditions to ensure compliance with global policies, and the detection of any violation of such, should also be set. International legal regime is the ultimate goal, and will ensure that penalization for the breaching of obligations will be prompt and effective (Evans, Kawaguchi, 2009).

Clausewitz stressed the importance of diplomacy throughout the conduct of war. There should be a careful design established between upholding and in fact ameliorating diplomatic relationships and sustaining or propagating active defense. Nowadays, capabilities of state and non-state actors are such that the counterpart automatically feels itself threatened without purpose. Long-term damage not only in physical or virtual terms, but also in domestic image and international relations should be considered when devising an action plan. A careless act may result in the disturbance of economic, social, cultural and political ties. The usage of all necessary means- diplomatic, informational, military and economic- is crucial.

Private and Public Sector

Public-private partnerships have to be established to ensure higher security, integrity and availability. This will also

build collective self-defenses and will maintain a common operating picture (US DoD, 2011). Such partnership has to be based on open, trustworthy and innovative programs of cooperation.

One of the challenges posed by the securitization of cyberspace is the parallel respect of principles of privacy, free flow of information and other fundamental freedoms (US DoD, 2011; White House, 2011). At the same time it is crucial to maintain the human rights and privacy standards, which could be easily put at stake when national security is targeted. The major debate raised is the freedom of expression and of information. However, here one may argue that typically, the freedom stays unless it threatens national security. A draft bill has been submitted to the UK recently, which will allow the storage of all communication information- who, where and when- but not the content of such interaction (Brewster, 2012).

Establishing collateral damage as a result of a cyber attack is certainly referring to the physical world consequences of the attack on, for example, an electric power grid. In such a case, a government's policy, including deterrence, may weaken private sector's incentive to protect its own systems. Any policy that hints that a cyber attack is an act of war or terrorism tends to immunize infrastructure owners against such a risk, when they tend to claim force majeure. But this reduces political pressure to protect their systems (Libicki, 2009). A law regulating the inter-agency and government collaboration and insurance against cyber terrorist attacks may be a good starting point in building a platform for cooperation and exchange of expertise and information.

International cooperation is another key aspect in targeting cyber threats more efficiently. The policies in this field may vary dramatically between two countries in inter-state cybersecurity challenges. Safeguarding US and global interests using economic tools, by creating and promoting common standards for the international trade of soft and hardware will build not only mutual trust, but will directly address terrorist threats. Initiating dialogues and sharing best practices will increase the capacity of individual states and collective enterprises. Dissuasion by strength at home and abroad should be initiated by the whole of government in collaboration with the private sector and individual citizens. Technological innovation should be invested in. People, technology, research and development are major fields for sustainable capabilities at national security levels. "Globally distributed early warning capabilities" and assistance to less developed nations in building their capacities is a constructive and beneficial undertaking as for domestic, so for international profit (White House, 2011).

The current absence of a centralized authority- or a link between authorities- puts all the pressure of the control of network infrastructure on private entities. Promoting communication between law enforcement and service providers regarding evidence gathering, data retention and privacy concerns will put relationships on a higher level and will make cooperation more efficient. Regular meetings, joint training and informal relationship and trust-building sessions between the public and private sectors should be initiated by appropriate bodies (Miedico, 2012).

Initiatives of International Organizations

Neorealists sustain that, as threats may arise from state, as well as non-state actors, international institutions should provide a forum for international cooperation; although even they alone cannot guarantee security (Alexander, 2007). But something is better than nothing, and, with efforts, a lot more can be achieved.

The UN, as the keeper of international peace, began a project on a cyber treaty back in 2005. UNODC, as the primary specialized agency for technical and legislative assistance to Member States on terrorism has initiated a publication on "The Use of Internet for Terrorist Purposes" in 2012, along with guidance on cybercrime. A global, sustainable and holistic approach through an integrated framework includes the training for relevant personnel- as legal, so investigative and technical- the development of legal tools, the strengthening of cooperation, enhancing prevention and awareness raising, data collection, research and analysis (Miedico, 2012). Harmonization of international and national legal instruments, building legal expertise in specialized areas, making sure to link different spheres of terrorism and other threats for a global picture is what the UNODC undertakes (Miedico, 2012). Public awareness, investment in education, scientific research, and development of cyber law have all been initiated although not on a sufficiently broad and, indeed, narrow level, to be able to address global and more specific problems.

When Kofi Annan urged the UN to act more preventively than reactively, he aimed at addressing the deep-rooted structural causes of conflict (Crawford, 2007). Sensibility, mutual understanding and trust should be the primary preoccupation in this policy. And the UN is reviving this approach in application to cyber terrorism through ongoing projects.

Universal counter-terrorism instruments and UN Security Council Resolutions 1373, 1566, 1624 and 1963 all aim at preventing, addressing and judging terrorism cases in a global manner. These instruments, easily applied to the virtual world, should be supplemented by more appropriate to the domain instruments (UNODC, 2012).

The EU has also recently launched the Critical Information Infrastructure Protection Initiative outlining the tasks and actions (Gable, 2009). The European Convention on Cybercrime is the only agreement, albeit regional and narrow, that addresses cyber attacks directly. Nevertheless, it is a very influential body of customary law and a good scheme for possible future developments (Carr, 2012; Schjolberg, 2010).

Although limited to NATO-Member States, the formulation of the 2010 Strategic Concept elaborates ideas that can be put into practice in relation to all countries

“using the [NATO] planning process to enhance and coordinate national cyber-defence capabilities, bringing all [NATO] bodies under centralized cyber protection, and better integrating [NATO] cyber awareness, warning and response with member nations” (NATO, 2010).

However, for NATO to resourcefully defend the cyber domain, it must improve its ability to prevent, detect, counter and recover from cyber attacks by setting technical, military and political priorities (Geers, 2011). It should also build and enhance military alliances and tactics to confront potential threats in cyberspace- deterrence and response has never been such an acute necessity. As a military organization, it should ensure that adversary cyber reconnaissance should be made as difficult as possible and future technology is targeted at its source.

Building technical capacity and enhancing national-level cyber security among developing nations is of immediate and long-term benefit, as States are equipped with dealing with threats emanating from within their borders. To “deny terrorists … the ability to exploit the Internet for operational planning, financing, or attacks” and to “recognize and adapt to the military’s increasing need for reliable and secure networks” is not only the task of national governments, but of international institutions as well (White House, 2011).

The technical and forensic sides should be separated as much as possible from the legal and political ramifications- and that may be achieved through clearly set mandates of international organizations (Geers, 2011). Geopolitical knowledge is critical, and international organizations can collect, evaluate and transmit digital evidence to appropriate bodies or States for a sound approach (Geers, 2011).

International organizations should act as forum in bringing together States and other organizations to be able to collaborate immediately through treaties, devise new technical tools and develop policies. Civil society and NGOs should be engaged to establish safeguards, among other set tasks. International organizations can promulgate information security standards and industry can be encouraged to implement them (ITU, 2005). Through an institutional framework, it is essential to

“promote cyberspace cooperation, particularly on norms of behaviour for states and cybersecurity, bilaterally and in range of multilateral organizations and multinational partnerships” (White House, 2011).

Critical Infrastructure Strategy

As Deputy Secretary of Defence Ashton B. Carter put it in March 2012, “I dare say, we’d spend a lot more if we could figure out where to spend it”.

Critical infrastructure should be appropriately secured and technically developed in order to withstand to the

maximum possible to any external intrusions. Whilst international organizations should promote cooperation on a global level, and more general approaches to resolving cyber security threats, national governments are responsible for the technical amelioration of capabilities.

Unlike a conventional attack, cyber attacks should be stopped ex ante. This would act as a barrier to prevention of further attacks and the motivation of the enemy to act illegally. Early detection and warning programs will detect cyber attacks in mid-attack, which, however, makes it more difficult to classify (Carr, 2012). Mitigating the above risks may be done by strengthening workforce communications, accountability, internal and personnel monitoring and information management capabilities (US DoD, 2011). New concepts and architectures should be developed, including a comprehensive active cyber defense capability, which will strengthen the systems and networks. By this, real-time capability of discovering, detecting, analyzing and tracking the threats will enhance using sensors software and intelligence (US DoD, 2011).

Computer network defense is the primary target to address in a policy. Creating a separate secure network with integrated security for the specific use of critical infrastructure systems with large scale monitoring is a potential strategy. Information warfare, psychological applications, military deception, operations security and electronic warfare are used as the core capabilities for command and control.

The core challenges include attribution, situation awareness, lack of common taxonomy, information sharing, and system integration. Technically, mobile devices, resilience, chain of trust and data protection are amongst the most difficult issues to be resolved (Andress, Winterfeld, 2011). The strategy developed by DoD relates cyberspace to an operational domain. With a special division of CYBERCOM, the DoD aims to manage cyber risks through increased training, information exchange and creation of secure network environments (US DoD, 2011). A good initiative, it has yet to be developed to the fullest potential and the US has to devote more personnel and resources to the cyber domain, training a greater number of skilled forces (Carr, 2012: p.194). The US Computer Emergency Readiness Team has publicized a great deal of advice on how to tackle attacks. However, administrators do not have the time to absorb this (Geers, 2011).

Developing threat scenarios for risk management, resiliency, recovery plans and prioritization is one possible approach. From this perspective, a range of mechanisms can be used to mitigate the risks. The management framework could be a cycle comprising system authorization, control monitoring, security categorization, security control selection, refinement, documentation, implementation and assessment (Andress, Winterfeld, 2011). Vulnerability assessment indicates the capabilities of actors and opportunities to act, while security controls testing protocols ensure effective protection of information infrastructure (Carr, 2012). An interrelated set of tasks it is an essential stance in which the government should be fully involved. Emergency communication, control and management, as well as capturing forensic data may increase centralized protection.

Increasing the performance of critical infrastructures allows them to become more vulnerable to cyber and physical attacks. Academia and industry collaboration ensures an appropriate exchange of practice and technical expertise for the securitization of systems in specialized fields, such as that of the high-tech supply chain. Objective threat evaluation and suitable resource allocation, with investment in network security and incident response is suggested by Geers (2011).

Another possible advancement in the field is the identification and regulation of patterns and players. IPv6 may increase attribution by lowering anonymity, but there is a long and dangerous transition phase. Individual, speedy and incremental development of specifically targeted protection mechanisms is a worthwhile investment (US DoD, 2011).

A long-term goal, it requires technological sophistication and is influenced by the impact of different national regulations on data control. At this moment, the importance of formal and informal channels of cooperation, and the development of relationships of trust in handling sensitive information between the public and private sector springs up (Miedico, 2012). Cross-border cooperation with national authorities to leverage direct, informal relationships with the private sector service providers may be recommended as an alternative to the hitherto developing individual

technical expertise.

Conclusion

This paper has summarized the main current thoughts in the field, debates and probable outcomes, taking into consideration political theories, such as discourse analysis, Sun Tzu's theory of war, and doctrines of the US Department of State. The current fundamentalist interpretations of the Quran have been said to influence the emergence of the cyber domain as the domain for 'jihad' and extremist activity of all kinds.

A long-standing debate on the definition of cyber terrorism and the application of the legal domain to the current situation has not been resolved. Yet, applying Aristotle's epistemology may help to reach a satisfactory definition, which in turn may help develop a fitting convention. Possible solutions for policy-makers and legislators have been outlined, with consideration of issues that arise in politics, economics and among the society. Legal initiatives, through national channels and international organizations have to be initiated or pursued in order to attain the development of an international cyber treaty addressing terrorism.

To compile a policy that would be able to respond not only to today's needs and problems, but would also look into the future possible activities in the cyber domain, the government has to research and analyze all the multi-disciplinary aspects of the cyber domain. Of a great importance is international cooperation, which has to be set as a long term goal, with negotiation of mutually acceptable benchmarks. Short and long term policy goals have to be set, monitored and implemented. Overall, an integrated approach may help mitigate risks, improve on policies and acquire capabilities that would resolve any potential conflict in the virtual world.

References

Abdel Haleem, A.M.S (2008) *The Qur'an*, Oxford World's Classics

Adams, James (2001) 'Virtual defense', *Foreign Affairs 80(3)* p.98-112

Aitoro, Jill R. (2009) *Terrorists nearing ability to launch big cyberattacks against US* http://www.nextgov.com/technology-news/2009/10/terrorists-nearing-ability-to-launch-big-cyberattacks-against-us/44951/ Accessed 20.7.2012

Albanesius, Chloe (2012) *FBI Director: cyber attacks could be bigger threat than terrorism* http://www.pcmag.com/article2/0,2817,2401083,00.asp Accessed 29.7.2012

Alexander, Gerard (2007) 'International Relations Theory Meets World Politics: the Neoconservative vs. Realism debate' in *Understanding the Bush Doctrine: Psychology and Strategy in an Age of Terrorism,* edited by Peter Suedfeld and Stanley Renshon, p. 39-59. New York: Routledge, 2007

Al Jazeera (2012) *The online arms race: is the threat of cyber war more hype than reality?* http://stream.aljazeera.com/story/online-arms-race-0022228 Accessed 30.6.2012

Andress, Jason and Winterfeld, Steve (2011) *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioner*, Syngress

Aristotle (2008) *Logics and the theory of knowledge (epistemology)* http://prepod.info/ru/article/logika-i-teoriya-poznaniya-epistemologiya-aristotelya/ Accessed 5.8.2012

Atayf, Mohamad (2012) *Scholars speak out in favor of "electronic Jihad" against the enemy* http://english.alarabiya.net/articles/2012/01/29/191307.html Al Arabiya, Accessed 20.7.2012

Baker, Steward and Dunlap, Charles (2012) 'What is the role of lawyers in cyberwarfare?'*ABA Journal*, May 2012 http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/ Accessed 21.7.2012

Baldor, Lolita (2012) *Pentagon still grappling with rules of cyberwar* http://www.federalnewsradio.com/394/2961646/Pentagon-still-grappling-with-rules-of-cyberwar- Accessed 28.7.2012

Bell, D. S. A. 'International relations: the dawn of a historiographical turn?' *British Journal of Politics and International Relations* 3:1 (2001), pp.115-126

Bernama (2012) *ASEAN and Japan enter new phase in counter-terrorism efforts* http://www.bernama.com/bernama/v6/newsgeneral.php?id=684593 Accessed 31.7.2012

Betz, David (2012) *Cyberpower and International Security*, Foreign Policy Research Institute E-notes, June 2012

Brewster, Tom (2012) *NATO: cyber terrorism not yet a real threat* http://www.techweekeurope.co.uk/news/nato-cyber-terrorism-84942 Accessed 22.7.2012

Brust, Richard (2012) 'Cyberattacks: computer warfare looms as next big conflict in international law', *ABA Journal*, May 2012, p.40-45

Buchanan, Allen (2007) 'Justifying Preventive War' in Shue, Henry and Rodin, David *Preemption: Military Action and Moral Justification*, Oxford University Press; p. 126-142

Buckley, Mary and Singh, Robert (2006) *The Bush Doctrine and the War on Terrorism,* Routledge

Bunt, Gary (2003) *Islam in the digital age*, Pluto Press

Carr, Jeffrey (2012) *Inside cyber warfare*, O'Reilly, 3rd Edition

Clarke, Richard; Knake, Robert (2010) 'Cyber war' in Harper, Collins;

Coleman, Kevin *Cyber Terrorism* Computer Crime Research Centre http://www.crime-research.org/library/Cyberterrorism.html Accessed 29.7.2012

Joint Paper (2012) *Russia's 'Draft Convention on International Information Security': a commentary,* Conflict Studies Research Centre and Institute of Information Security Issues, Moscow State University

Conway, Maura (2006) 'Terrorism and the internet', *Parliamentary Affairs* 59(2), p. 283-298

Cox, Michael and Stokes, Doug (2012) *US Foreign Policy*, 2nd edition, Oxford University Press

Crawford, Neta (2004) 'Understanding discourse: a method of ethical argument analysis' *Qualitative Methods* 2:1 (2004): 22-25

Crawford, Neta (2007) 'The false promise of preventive war: the 'new security consensus' and a more insecure world' in Shue, Henry and Rodin, David *Preemption: Military Action and Moral Justification*, Oxford University Press; p. 89-125

Davis, Paul and Jenkins, Brian Michael (2002) *Deterrence and influence in counterterrorism: a component in the war on Al Qaeda*, Rand Corporation, US

Denning, Dorothy (2002) 'Activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy', in Arquilla, J. & Ronfeldt, D. *Networks and netwars: The Future of Terror, Crime, and Militancy,* RAND Corporation, Ch. 8, p.239-288

DSCINT (2006) *Handbook No. 1.02: Cyber Operations and Cyber Terrorism*, US Army Training and Doctrine Command

Dunlap, Charles (2011) 'Perspectives for cyber strategists on law for cyberwar', *Strategic Studies Quarterly,* spring 2011 p. 81-99 http://www.au.af.mil/au/ssq/2011/spring/dunlap.pdf Accessed 21.7.2012

Evans, Gareth and Kawaguchi, Yoriko (2009) *Eliminating nuclear threats: a practical agenda for global policymakers, synopsis,* International Commission on Nuclear Non-proliferation and Disarmament

Fars News Agency (2012a) *Tehran Anti-Terror Conference Ends Work with Final Statement* http://english.farsnews.com/newstext.php?nn=9004052538 Accessed 22.7.2012

Fars News Agency (2012b) *US expanding cyber attack capability to sabotage other nations' facilities* http://english.farsnews.com/newstext.php?nn=9104250254 Accessed 22.7.2012

FBI (2002) *Terrorism 2002-2005*, US Department of Justice

Financial Times (2011) *The case for cyberdefence* http://www.ft.com/intl/cms/s/0/f6f3c114-8d48-11e0-bf23-00144feab49a.html#axzz1ynGbk03I Accessed 12.06.2012

Finkle, Jim (2012) *Another cyber espionage campaign found targeting Iran* http://www.reuters.com/article/2012/07/17/net-us-cybersecurity-middleeast-idUSBRE86G0M320120717 Accessed 29.7.2012

Finlan, Alastair (2006) 'International Security' in Buckley, Mary and Singh, Robert *The Bush Doctrine and the War on Terrorism: Global Responses, Global Consequences.* London and New York: Routledge, pp. 150-163

Finnis, John and Boyle, Joseph (1988) *Nuclear Deterrence, Morality and Realism*, Clarendon Press, Oxford

Focus News Agency (2012) *General Todor Boyadzhiev: threat of cyber terrorism is growing steadily* http://www.focus-fen.net/index.php?id=n283620 Accessed 21.7.2012

Gable, Kelly (2009) 'Cyber-apocalypse now: securing the internet against cyberterrorism and using universal jurisdiction as a deterrent', *Vanderbilt Journal of Transnational Law Vol. 43:57*, p.57- 118

Gasper, Peter (2008) *Cyber threat to critical infrastructure,* Idaho National Laboratories http://usacac.army.mil/cac2/cew/repository/presentations/15_Idaho_Natl_Lab_IACS-CI_Threat_2010-2015.pdf Accessed 22.7.2012

GCN (2012) *DoD wants cyberterrorism-prediction software* http://gcn.com/articles/2012/07/31/agg-dod-small-biz-software-support.aspx Accessed 1.8.2012

Geers, Kenneth (2010a) "Cyber Weapons Convention", *Computer Law and Security Review* 26(5), p. 547-551

Geers, Kenneth (2010b) *Arms control in cyberspace: a proposal* http://www.internetevolution.com/author.asp?section_id=628&doc_id=201773 Accessed 22.7.2012

Geers, Kenneth (2011a) *Strategic cyber security*, NATO Cooperative Cyber Defence Centre of Excellence

Geers, Kenneth (2011b) *Sun Tzu and cyber war,* NATO Cooperative Cyber Defence Centre of Excellence 1-23

Geller, Pamela (2012) *Islamic scholars approve e-jihad and cyber warfare* http://atlasshrugs2000.typepad.com/atlas_shrugs/2012/01/islamic-scholars-approve-e-jihad-and-cyber-

warfare.html Accessed 20.7.2012

Gellman, Barton (2002) *Cyber-attacks by Al Qaeda feared; terrorists at threshold of using internet as tool of bloodshed, experts say*, Washington Post, June 27, 2002, at A01.

Giles, Keir (2012) *Russia's public stance on cyberspace issues*, Conflict Studies Research Centre, UK http://www.conflictstudies.org.uk/files/Giles-Russia_Public_Stance.pdf Accessed 29.7.2012

Goodman, Seymour and Kirk, Jessica and Kirk, Megan (2007) 'Cyberspace as a medium for terrorists', *Technological Forecasting and Social Change*, Vol. 74, No. 2, pp.193-210

Gordon, Sarah and Ford, Richard (2011) *Cyberterrorism?* Symantec Security Response, White Paper

Gorman, Siobhan and Barnes, Julian (2011) 'Cyber combat: act of war'*, Wall Street Journal,* May 31 2011

Greenemeier, Larry (2007) *'Electronic jihad' app offers cyberterrorism for the masses* http://www.informationweek.com/news/200001943 Accessed 17.7.2012

Gray, David and Head, Albon (2009) 'The importance of the internet to the post-modern terrorist and its role as a form of safe haven' *European Journal of Scientific Research* 25(3) p.396-404

Guneev, Sergey (2012) '*End of the world as we know it': Kaspersky warns of cyber-terror apocalypse* http://www.rt.com/news/kaspersky-fears-cyber-pandemic-170/ Accessed 8.8.2012

Gurtov, Mel (2006) *Superpower in crusade: the Bush Doctrine in US Foreign Policy*, Lynne Rienner, US

Hakken, David (2003) *The Knowledge Landscapes of cyberspace*, Routledge, London

Handel, Michael (1991) *Sun Tzu and Clausewitz compared*, Strategic Studies Institute, US Army War College.

Hansen, James V. and Lowry, Paul Benjamin and Meservy, Rayman and McDonald, Dan (2007) *Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection*, Decision Support Systems (DSS), vol. 43(4), pp. 1362-1374

Harris, Shon (2010) *All-in-One CISSP,* McGraw-Hill Companies

Hatamoto, Michael (2012) *FBI: beware of terrorist cyber attacks,* Daily Tech http://www.dailytech.com/article.aspx?newsid=24246 Accessed 29.7.2012

Hathaway, Melissa (2009) *Securing our digital future,* The White House Blog http://www.whitehouse.gov/CyberReview Accessed 28.7.2012

He-Suk, Choi (2012) *N.Korea has third most powerful cyberwar capabilities* http://www.stripes.com/news/pacific/n-korea-has-third-most-powerful-cyberwar-capabilities-1.179826 Accessed 29.7.2012

Holmes, Robert (1992) 'Can war be morally justified? The Just War theory' in Elshtain, Jean Berthke *Just War Theory*, NYU Press, p. 197-233

Homeland Security News Wire (2010) *A first: 15 nations agree to start working together on cyber arms control* http://www.homelandsecuritynewswire.com/first-15-nations-agree-start-working-together-cyber-arms-control Accessed 28.7.2012

Hoover, Nicholas (2012) *Cyber attacks becoming top terror threat, FBI says*

http://www.informationweek.com/news/government/security/232600046 Accessed 29.7.2012

Hopf, Ted (2004) 'Discourse and content analysis: some fundamental incompatibilities' *Qualitative Methods* 2:1 (2004): 31-33

Hopkins, Curt (2011) *Sudan lauches a cyber-army wrapped in the Koran* http://www.readwriteweb.com/archives/sudan_wraps_cyber-army_in_the_koran.php Accessed 17.7.2012

Horwitz, Sari (2012) *Justice Department trains prosecutors to combat cyber espionage,* Washington Post http://www.washingtonpost.com/world/national-security/justice-department-trains-prosecutors-to-combat-cyber-espionage/2012/07/25/gJQAoP1h9W_story.html Accessed 28.7.2012

Hoyos, Carola (2012a) *Defence groups move to cybersecurity* http://www.ft.com/intl/cms/s/0/1c406986-6b10-11e1-9781-00144feab49a.html#axzz1ynGbk03I Accessed 11.6.2012

Hoyos, Carola (2012b) *NATO to begin cyber security drive* http://www.ft.com/intl/cms/s/0/7afcaa96-6243-11e1-872e-00144feabdc0.html#axzz21GAUmVyG Accessed 21.7.2012

Hughes, Christopher (2004) 'Controlling the internet architecture within Greater China' in Mengin, Françoise *Cyber China: Reshaping National Identities in the Age of Information,* Palgrave Macmillan, p. 71-90

ICJ Advisory Opinion (1996) 'Legality of the threat or use of nuclear weapons', *Reports* p.226-267

Ignatieff, Michael (2004) *The lesser evil: political ethics in an age of terror*, Edinburgh University Press

Inquisitr (2012) *Pentagon wants to monitor Twitter and Facebook activity to prevent 'cyber terrorism events'* http://www.inquisitr.com/288515/pentagon-wants-to-monitor-twitter-and-facebook-activity-to-prevent-cyber-terrorism-events/ Accessed 1.8.2012

International Commission on Intervention and State Sovereignty (2001) *The Responsibility to Protect*, Ottawa International Development Research Centre

Islamic Republic of Iran (1991) *Penal Code*

ITU (2005) *A comparative analysis of cybersecurity initiatives worldwide,* WSIS Thematic Meeting on Cybersecurity

Jaycox, Mark (2012) *The Cybersecurity Act was a surveillance bill in disguise* http://www.guardian.co.uk/commentisfree/2012/aug/02/cybersecurity-act-surveillance-bill-disguise Accessed 18.8.2012

Jervis, Robert (2005) *American Foreign Policy in a new era*, Routledge, London

Johnson, James Turner (1992) 'Threats, values and defense: does the defense of values by force remain a moral possibility?' in Elshtain, Jean Berthke *Just War Theory*, NYU Press, p. 55-76

Jordan, Tim (2008) *Hacking: digital media and technological determinism*, Polity Press, Cambridge, UK

JP 1-02 (2010) *Department of Defence dictionary of military and associated terms*, US

JP 3-13 (2006) *Information Operations*, US

Kroft, Steve (2012) *Stuxnet: computer worm opens new era of warfare* http://www.youtube.com/watch?v=6WmaZYJwJng Accessed 5.8.2012

Laffey, M. and Weldes, J. (2004) 'Methodological reflections on discourse analysis', *Qualitative Methods* 2:1 (2004): 28-31

Lee, Robert (2012) *Stuxnet and cyber deterrence* http://www.infosecisland.com/blogview/22168-Stuxnet-and-Cyber-Deterrence.html Accessed 13.8.2012

Lele, Ajey (2012) *Pakistan's 'other options' on display* http://www.dailypioneer.com/columnists/item/52192-pakistan%E2%80%99s-%E2%80%98other-options%E2%80%99-on-display.html Accessed 11.8.2012

Levin, Adam (2012) *Congress' profound failure on Cybersecurity* http://abcnews.go.com/Business/congress-profound-failure-cybersecurity-care/story?id=16979814#.UCYzDqPAG7s Accessed 11.8.2012

Levy, Jack (2007) 'Preventive war and the Bush Doctrine: theoretical logic and historical roots' in Stanley A. Renshon and Peter Suedfeld *The Bush Doctrine: Psychology and Strategy in an Age of Terrorism*, London: Routledge, Pp. 175-200

Lewis, James Andrew (2002) *Assessing the risks of cyber terrorism, cyber war and other cyber threats,* CSIS, Washington DC

Lewis, James Andrew (2007) 'Cyber security as a national and international issue in governance' in Banerjee, Indrajit *The internet and governance in Asia: a critical reader*, AMIC, p.217-238

Lewis, James Andrew (2008) *Securing Cyberspace for the 44th Presidency*, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, CSIS Washington DC

Lewis, James Andrew (2010a) *Multilateral agreements to constrain cyberconflict,* Arms Control Today, June 2012

Lewis, James Andrew (2010b) *The cyber war has not begun,* CSIS, Washington DC

Liaropoulos, Andrew (2011) *Cyber-security and the law of war: the legal and ethical aspects of cyber-conflict,* GPSG Working Paper #7

Libicki, Martin C. (2009) *Cyberdeterrence and cyberwar*, RAND Project Air Force

Lourdeau, Keith (2004) *Virtual Threat, Real Terror: Cyberterrorism in the 21st Century,* Testimony: United States Senate Committee on the Judiciary http://www.iwar.org.uk/cyberterror/resources/ct-hearing/lourdeau.htm Accessed 30.6.2012

Luban, David (2007) 'Preventive War and Human Rights' in Shue, Henry and Rodin, David *Preemption: Military Action and Moral Justification*, Oxford University Press; p. 171-201

Markoff, John and Kramer, Andrew (2009) *In shift, U.S. talks to Russia on internet security* http://www.nytimes.com/2009/12/13/science/13cyber.html?_r=3 Accessed 22.7.2012

McElroy, Damien (2012) *Flame virus 'has infected 189 systems in Iran'* http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9297703/Flame-virus-has-infected-189-systems-in-Iran.html Accessed 21.7.2012

McNeal, Gregory (2007) 'Cyber embargo: countering the internet jihad' *Case Western Reserve Journal of*

International Law Vol.39, p.789-827

Memri TV (2011) *Kuwaiti Islamist preacher Tareq Sweidan, manager of Al-Resala TV, calls for armed resistance and electronic jihad against Israel* http://www.memritv.org/clip/en/2980.htm Accessed 21.7.2012

Menn, Joseph (2011) *Agreement on cybersecurity 'badly needed'* http://www.ft.com/intl/cms/s/0/e595e568-f4dc-11e0-ba2d-00144feab49a.html#axzz1ynGbk03I Accessed 24.6.2012

Messmer, Ellen (2012a) *U.S. seeking to build international unity around cyberdefense for industrial control systems* http://www.pcadvisor.co.uk/news/security/3357075/us-seeking-build-international-unity-around-cyberdefense-for-industrial-control-systems/ Accessed 30.6.2012

Messmer, Ellen (2012) *Black Hat: cyber-espionage operations vast yet highly focused, researcher claims* http://www.networkworld.com/news/2012/072512-blackhat-stewart-261126.html?hpg1=bn Accessed 28.7.2012

Middle East Online (2012) *Cyber war: 'Gaza hackers' deface Israel fire service website* http://www.middle-east-online.com/english/?id=49991 Accessed 26.7.2012

Miedico, Mauro (2012) *Assisting Member States in preventing and detecting the use of internet for terrorist purposes,* UNODC Terrorism Prevention Branch, Vienna, Austria

Milliken, J. (1999) 'The study of discourse in international relations: a critique of research and methods' *European Journal of International Relations*, 5: 2, 225-254.

Nakashima, Ellen (2011) *List of cyber-weapons developed by Pentagon to streamline computer warfare* http://www.washingtonpost.com/national/list-of-cyber-weapons-developed-by-pentagon-to-streamline-computer-warfare/2011/05/31/AGSublFH_story.html Accessed 28.7.2011

Natan, Yoel (no date) *164 Jihad verses in the Koran* http://www.answering-islam.org/Quran/Themes/jihad_passages.html Accessed 18.8.2012

NATO (2010) *Active engagement, modern defence: strategic concept for the defence and security of the members of the North Atlantic Treaty Organization* http://www.nato.int/cps/en/natolive/official_texts_68580.htm Accessed 20.7.2012

NATO (2010) *NATO 2020: assured security; dynamic engagement* http://www.nato.int/cps/en/natolive/official_texts_63654.htm Accessed 31.7.2012

NATO (2011a) *Cyber defence: next steps* http://www.nato.int/cps/en/SID-D038B864-77192245/natolive/news_75358.htm?selectedLocale=en Accessed 31.7.2012

NATO (2011b) *Working with the private sector to deter cyber attacks* http://www.nato.int/cps/en/SID-D038B864-77192245/natolive/news_80764.htm?selectedLocale=en Accessed 31.7.2012

NATO (2012) *NATO and cyber defence* http://www.nato.int/cps/en/SID-FDAB2840-D18562F4/natolive/topics_78170.htm Accessed 31.7.2012

Nau, Henry (2003) 'Identity and the balance of power in Asia' in Ikenberry, John and Mastanduno, Michael *International Relations Theory and the Asia Pacific*, Columbia University Press: p.213-242

Naughton, John (2012) *Cyberwarfare takes Heidegger's ideas to their logical end* http://www.guardian.co.uk/technology/2012/apr/01/cyberwarfare-unmanned-drones-heidegger Accessed 20.6.2012

Parks, Raymond and Duggan, David (2001) *Principles of cyber-warfare,* Proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001

PCCIP (1997) *Critical foundations: protecting America's infrastructure,* The Report of the President's Commission on Critical Infrastructure Protection, US

Perlroth Nicole (2012) *Unable to crack computer virus, security firm seeks help* http://bits.blogs.nytimes.com/2012/08/14/unable-to-crack-computer-virus-security-researchers-issue-cry-for-help/ Accessed 17.8.2012

Petallides, Constantine (2012) *Cyber terrorism and IR theory: realism, liberalism, and constructivism in the New Security Threat,* StudentPulse Vol. 4 No. 3 http://www.studentpulse.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat Accessed 20.7.2012

Pollitt, Mark (1997) *Cyberterrorism- fact or fancy?* http://www.cs.georgetown.edu/~denning/infosec/pollitt.html Accessed 21.7.2012

Protalinski, Emil (2012) *Former Pentagon analyst: China has backdoors to 80% of telecoms* http://www.zdnet.com/former-pentagon-analyst-china-has-backdoors-to-80-of-telecoms-7000000908/ Accessed 29.7.2012

Provan, Jonathan (2012) *Is the United States a 'Neocon Nation'?* http://www.e-ir.info/2012/03/09/is-the-united-states-a-neocon-nation/ Accessed 28.7.2012

Renshon, Jonathan (2007) 'The psychological origins of preventive war' in Peter Suedfeld and Stanley Renshon *Understanding the Bush Doctrine: Psychology and Strategy in an Age of Terrorism,* p. 201-230, New York: Routledge

Rezvaniyeh, Farvartish (2010) *Pulling the strings of the net: Iran's cyber army* http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html#ixzz21T1J0vb2 Accessed 28.7.2012

Rockmore, Tom (1997) On Heidegger's Nazism and philosophy, University of California Press

Russia Today (2012) Stuxnet, Flame…Gauss: New spy virus found in Middle East http://rt.com/news/gauss-virus-stuxnet-flame-276/ Accessed 18.8.2012

Sanchez, Mary (2012) *What should come first, partisan advantage or national security?* http://www.sacbee.com/2012/08/03/4689456/mary-sanchez-what-should-come.html Accessed 4.8.2012

Schjolberg, Judge Stein (2011) 'Wanted: a United Nations cyberspace treaty' in Nagorski Andrew *Global Cyber Deterrence: views from China, the US, Russia, India and Norway*, EastWest Institute, p.11-14

Schmidt, Howard (2011) *Launching the US international strategy for cyberspace,* The White House Blog http://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace Accessed 28.7.2012

Schmitt, Michael (1999) 'Computer Network Attacks and the use of force in international law: thoughts on a normative framework' *Columbia Journal of Transnational Law 37(1999) 885*, p. 889-937

Senate (2012) *The Cybersecurity Act of 2012,* 112th Congress, 2nd Session, US

Shackelford, Scott (2009) 'From nuclear war to net war: analogizing cyber attacks in international law' *BJIL Vol.27 No.1*, p.191- 251

Sherill, Clifton (2012) 'Why Iran wants the bomb and what it means for US policy', *Nonproliferation Review, Vol. 19, No.1, March 2012*, p.31- 49.

Shue, Henry and Rodin, David (2007) 'The problem with prevention' in Shue, Henry and Rodin, David *Preemption: Military Action and Moral Justification*, Oxford University Press; p. 143-170

Shue, Henry (2007) 'What would a justified preventive military attack look like?' in Shue, Henry and Rodin, David *Preemption: Military Action and Moral Justification*, Oxford University Press; p. 222-246

Sidel, John (2012) *From cyberjihad to habermas: understanding Muslim identity and resistance online* http://blogs.lse.ac.uk/lsereviewofbooks/2012/06/18/book-review-islam-dot-com-contemporary-islamic-discourses-in-cyberspace/ Accessed 20.7.2012

Silverstein, Richard and Sahimi, Muhammad (2012) *Obama's virus wars: mutually assured cyber-destruction* http://www.guardian.co.uk/commentisfree/2012/jun/08/obama-virus-wars-mutually-assurred-cyberdestruction Accessed 30.6.2012

Stalinsky, Steven (2012) *Muslim Brotherhood restoration of caliphate and new era of cyber jihad* http://www.rightsidenews.com/2012061916452/world/terrorism/muslim-brotherhood-restoration-of-caliphate-and-new-era-of-cyber-jihad.html Accessed 20.7.2012

Tafoya, William (2011) *Cyber Terror,* FBI Law Enforcement Bulletin http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror Accessed 18.8.2012

Townshend, J. (2003) 'Discourse theory and political analysis: a new paradigm from the Essex School?' *The British Journal of Politics and International Relations* 5: 1, pp. 129-142

Tzu, Sun (2005) *The Art of War*, Shambala- Boston and London

United Nations (2005) *National Laws and Regulations on the prevention and suppression of international terrorism*, Part II, United Nations Legislative Series, New York

United Nations General Assembly Resolution 53/70 *Developments in the field of information and telecommunications in the context of international security*, Fifty-Third Session, Agenda Item 63

United Nations Office on Drugs and Crime (2012) *The use of internet for terrorist purposes,* United Nations, to be published autumn 2012

Uniacke, Suzanne (2007) 'On getting one's retaliation first' in Shue, Henry and Rodin, David *Preemption: Military Action and Moral Justification*, Oxford University Press; p. 69-88

US Department of Homeland Security (2011-2012) *Cyber storm: securing cyber space* http://www.dhs.gov/files/training/gc_1204738275985.shtm Accessed 2.7.2012

US Department of Defense (2011a) *Cyberspace Policy Report*, a Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934

US Department of Defense (2011b) *Department of Defense strategy for operating in cyberspace,* Washington

Vijayan, Jaikumar (2012) *No partisan fight over Cybersecurity bill, GOP senator says* http://www.pcadvisor.co.uk/news/security/3376511/no-partisan-fight-over-cybersecurity-bill-gop-senator-says/ Accessed 18.8.2012

Viotti, Paul and Kauppi, Mark (1999) *International Relations theory: realism, pluralism, globalism and beyond*, Allyn & Bacon.

Walker, Molly (2012) *Alexander: U.S. looking for offensive alternatives in cyberspace* http://www.fiercegovernmentit.com/story/alexander-us-looking-offensive-alternatives-cyberspace/2012-07-11 Accessed 29.7.2012

Weimann (2007) 'Virtual terrorism; how modern terrorists use the internet' in Banerjee, Indrajit *The internet and governance in Asia: a critical reader*, AMIC, p.189-216

Westby, Jody (2012) *Boards are still clueless about Cybersecurity,* Forbes http://www.forbes.com/sites/jodywestby/2012/05/16/boards-are-still-clueless-about-cybersecurity/ Accessed 30.6.2012

White House (2009) *The Comprehensive National Cybersecurity Initiative* http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf Accessed 29.6.2012

White House (2011) *International strategy for cyberspace: prosperity, security and openness in a networked world,* The White House, Washington

Wilson, Clay (2006) *Information Operations and cyberwar: capabilities and related policy issues* CRS Report for Congress

Xinhuanet News (2012) *Iran vows to counter any cyber attacks on nuclear facilities* http://news.xinhuanet.com/english/world/2012-07/26/c_131741432.htm Accessed 28.7.2012

—

Written by: Natalia Tereshchenko Written at: University of Durham
Written for: Dr. Vincent Keating
Date written: September 2012