# Cyber-Attacks Will Not Result in Armed Conflicts in the 21st Century

https://www.e-ir.info/2013/05/07/cyber-attacks-will-result-in-armed-conflicts-in-the-21st-century/

ASIM RIZVANOVIC, MAY 7 2013

**Cyber-Attacks Will Not Result in Armed Conflicts in the 21$^{st}$ Century. Discuss.**

There is a hysteria pervading international relations at the moment. The great hysteria of the Cold War was that of nuclear warfare, a threat questionably controlled by MAD (mutually assured destruction). The current hysteria is that of cyber-warfare and the threat that cyber-attacks pose to states. The difference between the two paradigms is essentially that nuclear strikes are evidently able to wipe out entire nations, but the power of cyber-attacks is far more ambiguous. Proponents argue that cyber-attacks will become kinetic in nature and actors will strike strategic or tactical targets in peace-time or during wars.

This essay offers a commentary upon these debates vis-à-vis asymmetry, the 'non-attribution' problem, and cyber-attacks themselves. The vast consensus is that asymmetry will allow states and non-state actors to conduct attacks disproportionate to their own conventional power; it is argued herein that this asymmetry, whilst factual to an extent, is somewhat limited to low-level attacks which are more a cause for annoyance than armed escalation. The 'non-attribution' problem dictates that victims of attacks will not be able to respond in kind nor escalate conflicts with any degree of confidence as to whom said responses should be directed towards. It is further argued that this is the main threat to 'cyber-peace'. The non-attribution problem is primarily an attractive aspect to lone actors who are merely able to cause annoyance and disproportionate financial costs. The totality of the argument set out in this essay will draw on the previous areas and highlight that whilst cyber-attacks are costly and can result in the direct loss of life, the overall zeitgeist that cyber-attacks are directly going to cause conflicts is over-hyped and generally incorrect. Furthermore, I argue that many of the proponents and lobbyists of militarising and further securing cyber-space are stakeholders who will directly benefit from the aforementioned actions.

The term 'weapon' is widely used in an incorrect form when talking about cyberspace. Traditionally, it has meant an instrument that is utilised to cause some kind of 'physical damage' to another object or person. Clearly then, an argument and context is mandatory for what constitutes a 'cyber-weapon', as the 'damage' it causes is of a different variety to that of a kinetic one. As Tabansky (2011, p. 81) states, "there is no common definition of 'cyber warfare' in the world". Further, Tabansky highlights a dangerous issue in the realm of international security, whereby what one country thinks constitutes espionage, another may deem it an actual 'act of war'. I concur with the 'cyber-weapon' definition proposed by Rid and McBurney (2012, p. 7):

"we understand a weapon as a tool that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things".

This argument rejects the concept of low-level viruses or other cyber-attacks geared towards economic espionage as weapons *per se*.

The tools at the disposal of a cyber-attacker range from very small scale programs which can essentially do no more than annoy the victim (such as low-level viruses), to much higher-end bespoke programs designed to cause actual physical damage to a person or property (such as the Stuxnet worm). The ease of creating a virus and infecting computers, or hijacking a computer remotely across continents means that cyber-warfare itself is asymmetric, but only to a degree. In 2001-2002, Gary McKinnon, a hacker from the UK, managed to infiltrate 97 US military and NASA systems from the his girlfriend's bedroom (BBC, 2008). Although the technology available to him, and that available to the US was starkly different McKinnon still managed to cause around $700 000 in damage (Parliament, 2008). This asymmetry is highlighted by many involved in the discussion, often comparing the paradigm of today with that of the Second World War, stating that both time periods favour offense as opposed to defence (Goldstein, 2010). The ease of acquiring a delivery system for cyber-attacks, in many cases a single computer (Lynn 2010, p. 98) further pushes cyber-warfare as an offense-favouring paradigm. Guy-Phillipe Goldstein, in his TED talk titled*How Cyber-Attacks Threaten World Peace* (2010), suggests that sixty years ago weapons such as aircraft and tanks favoured offense, thereby giving blitzkrieg a good chance of winning. Goldstein states that yet again the world is seeing a situation whereby offense is ahead of defence. Arguably, Goldstein is correct to some extent on matters of asymmetry, but his claims and arguments are exaggerated as a comparison of the*Stuxnet worm* and the *Sasser worm* demonstrate. These two particular cases are valid points of reference as Stuxnet is widely believed to be an Israeli-US joint project (Sanger, 2011), whilst the Sasser worm, one of the most wide spread worms of all time, was designed by a teenage boy in Germany (BBC, 2005). The cases highlight the actual disparity between government-sponsored offensives in comparison to the 'lone wolf'.

The Sasser worm was created by a boy in his bedroom and whilst it achieved significant annoyance and infection, (prominently including causing the delay of several transatlantic flights), its damage was nothing like that of a kinetic strike. Sasser was designed to spread through computer networks, whilst on the other hand Stuxnet was a tailored program designed for a specific goal: to delay the Iranian nuclear programme. Since its discovery, many security companies have investigated the source code. The most interesting thing about Stuxnet is that it searches for a specific factory environment. If it finds that it is 'inside' one then it executes its tasks; if it 'realises' it is not in a factory environment, then it does nothing (F-Secure, 2010). The investigation carried about by F-Secure (an I.T. security firm) highlights just how complex Stuxnet is, and their investigation resulted in an estimate that it would take a single person around 10 years to complete the coding (F-Secure, 2010).

The sheer complexity of Stuxnet and the fact that investigations have concluded it must have been created by a state or states goes some way in showing that cyber-attacks are not as asymmetric as is generally considered, especially when the two accused authors of the program, the USA and Israel, are perhaps the most advanced countries in the field of IT. Pondering the implications of Stuxnet and what it achieved further highlights this point. A vast amount of hours and cost went into its production, and the end result is merely a delay of the Iranian nuclear programme. Consider the damage that could have been caused by carrying out bombing raids, and consider the lesser amount of man-hours, and it is clear to see that cyber-attacks are still nowhere near as powerful as conventional attacks.

What Stuxnet, Sasser, and every form of 'malware', (software designed to damage computer systems) have in common is that they work by exploiting existing vulnerabilities in software, as Chen and Robert state "like biological viruses, computer viruses reproduce by taking advantage of the existing environment" (2004, p. 1). When a company creates software it is likely to be far from perfect and this is essentially how viruses and other forms of 'malware' can cause problems. This is very important in the asymmetry debate, as many who argue that asymmetry will cause conflicts, do not take into account that vulnerabilities are not fixed in time or space, nor are they universal. For a virus to work and execute a task such as to cause a power grid to go offline, a simple virus such as Sasser will not do, although it may cause temporary problems. For such complex infrastructure to be severely damaged, a program has to be 'intelligent' like Stuxnet, and to cause specific damage by taking advantage of vulnerabilities; as Libicki writes "there is, in the end, no forced entry in cyber space" (2009, p. 14). Libicki further suggests "organisations are vulnerable to cyberattack only to the extent that they want to be", his point being that in order to not get attacked, software must have zero vulnerabilities. The importance in what he states is that cyber-attacks can only exist against systems which have pre-existing vulnerabilities, with his argument showing that offense is not in charge; defence is. The role of an attacker is to find the gaps in the code, and the defender upon discovery of them, patches them up. This contradicts proponents who argue that cyber-war is advantageous to the attacker. The significance of this is that a program such as Stuxnet, whilst being effective in delaying the Iranian nuclear programme, will have almost no effect on another target, perhaps a hospital network, as the 'gap' the program would be looking to exploit will be totally different. Rid and McBurney make the same point, arguing that "target configurations are likely to be so specific that a powerful weapon may only be capable of hitting and acting on one single target…" (2012, p. 12). This means that cyber-weapons are not as asymmetric as we are lead to think, as they are simply not useful on a wide basis. The asymmetry theorem is further quashed when one considers that 'holes' in software render the offensive party in a weaker position than the defender, as weapons have a very limited time scope for being used; once they have been discovered the developer merely needs to correct the errors and therefore "exploits tend to depreciate rapidly after exposure" (Libicki, 2009, p. 157).

Of serious concern is the 'non-attribution' problem. This particular problem is not as easy to fix as a flawed piece of software, and in many cases may be impossible. Wheeler and Larson (2003, p. 1) define attribution as "determining the identity or location of an attacker or an attacker's intermediary", and expand the definition later to suggest

"all technical means for attribution are inherently limited. These limitations include attribution delay, failed attribution, and misattribution" (2003, p. 51).

The aforementioned technical limitations are what make cyber-crimes and cyber-attacks particularly attractive to those who seek to commit crimes or cause damage in one way or another. Whilst the technical limitations of attribution are abundant, there is hope that states will be put off using cyber-attacks as they will be unable to gain directly from them, as Glaser (2011, p.6) proposes,

"because states are driven by political motives, they will be unable to use countervalue cyber attacks to achieve their objectives without making known their identities"

Glaser (2011, p.6) also claims "the attribution problem may be less severe than is generally perceived"; a hollow and unfounded argument based on wishful thinking and an assumption that enemies are always rational. Whilst it is true that states will be unable to counter-value an attack politically, there may be states which are not particularly interested in doing so; they may simply want to cause damage to another without extracting a political victory. More dangerously, there may be states acting on behalf of other states, (perhaps without their knowledge), and it is this that makes the issue of attribution so dangerous.

A recent study titled *GPS Software Attacks* has shown that between 20% and 30% of the worldwide GPS system could be taken offline by a single attack (Nighswander *et al*, 2012, p. 8). Now considering the potential that a third-party could get involved in a conflict taking advantage of the difficulties of attribution, they could theoretically damage the GPS system as a way of supporting a favoured state. As a thought experiment, consider the US being at war with Iran. Russia could hack into the GPS system with just a single computer (Nighswander et al, 2012, p. 1), as a way of supporting Iran. This inherent danger makes it necessary for states to have a clear definition of what constitutes attack and what does not. The issue with defining cyber-attacks as acts of war is that it will be a large disincentive for developers and infrastructure owners to actually produce systems that are not full of security holes. Libicki explains this point coherently:

"any policy that stipulates that a cyberattack is an act of war (or even terrorism) tends to immunize infrastructure owners against such risks" (2009, p. 65).

The US has already hinted that such attacks may be seen as acts of war (Gorman and Barnes, 2011), and rather than setting limits to other states, they are creating a lax environment for their internal developers.

In 2007, Estonia was subjected to what is often inaccurately called 'cyber-war' (Traynor, 2007). Upon Russia's unleashing of "cyberwar to disable Estonia", as Traynor writing for *The Guardian* describes the events, many were quick to panic and overestimate the importance of the 'attacks'. Firstly, what constituted 'attacks' against Estonia was nothing like Stuxnet, nor was it in fact a virus or any kind of malware; it was what is called a 'Distributed Denial of Service Attack' (DDoS). Patrikakis, Masikos, and Zouraki describe a DDoS attack as

"a malicious attempt by a single person or a group of people to cause the victim, site, or node to deny service to its customers" (The Internet Protocol Journal, 2004).

Various actors were quick to begin campaigns calling for cyber-militarisation, urging NATO governments to invest in cyber-security, arguing that if Estonia could go down, so could anyone. This controversial argument was based on the fact that Estonia is one of the most well-connected societies in the world (Internet World Stats, 2012), ranking 28th overall. Estonia is just one rank behind the US (27th) in this data, and this particular dataset has been used to make the case that the DDoS attacks against Estonia were serious. Looking at the table again, one realises just how empty such facts are; for example, the Falkland Islands are ranked fourth, and it is very doubtful that Russia or China would be particularly worried about them. The importance of being 'well-connected' is exaggerated and confused with being powerful in the cyber realm. Referring to the alleged DDoS attack by Russia on Estonia, Gary McGraw questions "what would happen if you took that very attack and aimed at Google, or Amazon?" he continues, arguing, "absolutely nothing, they might not even notice" (Dartmouth, 2012). This goes some way in pointing out that many of the attacks we have seen thus far have not been dangerous. The most successful (known) attack is that of Stuxnet, and as I have highlighted earlier, the sheer complexity of the program means that as a result it is only really useful for one thing; attacking particular centrifuges in Iran.

To this day, the potential power of cyber-weapons is a great unknown, what Donald Rumsfeld would call a "known unknown" (US Department of Defense, 2002). The fact that cyber-power is so unquantifiable allows for many actors to voice differing arguments in favour of particular strategies. Take for example, Eugene Kaspersky the CEO of 'Kaspersky', a Russian I.T. security company. Kaspersky, in reference to on-going cyber-attacks, has stated, "I'm afraid it will be the end of the world as we know it, I'm scared, believe me" (Burt, 2012). Kaspersky stands to make a lot of money from security-issues in cyber-space; in fact his livelihood depends on it. For him and his company, they are not interested in inherently secure software and systems, as they are there to provide the security themselves, hence they can be described as cyber-vulnerability profiteers. In many cases Kaspersky is outright obvious in plugging his services, in one speech concluding, "better budgets on I.T. security is the solution for the problem" (Kaspersky, 2011). Kaspersky and other such companies are relying on the development of software that is far from perfect as they then are in a position to 'secure' said software. This misallocation of resources in the industry and the misallocation of economic incentives is what allows the proliferation of cyber-weapons. Rather than talking about deterrence, escalation and firewalls, there needs to be discussion about securing systems from the ground up, and that means developers have to be given 'carrots and sticks' in order to create software that is secure in the first place. Humans, unlike systems, do not operate on fixed parameters; hence it is just as important to educate staff on security protocols, as it is to secure the systems themselves. Making employees aware of 'social engineering' attacks, such as an attacker leaving a virus-laden flash-drive to be found and used by an employee, is vital also (Advanced Systems Group, 2010, p. 4).

After analysing the issues that generally are believed to offer asymmetric, offense-oriented, covert advantage, I believe that the world as a whole and particularly the US is in an excellent position to decrease system and software vulnerabilities. Although the ability is there, it is questionable as to whether the correct changes will be made to actually prevent armed-conflicts resulting from cyber-attacks. Michael Chirtoff, former secretary of Homeland Security, has commented,

"the concern you have, is that we are not going to take the hard decisions in this area until we have the equivalent of a Pearl Harbour or a 9/11" (Al-Jazeera, 2010).

Chirtoff has a point, the potential of a mass scale attack on the US may be possible, albeit unlikely, but such cyber-attacks would more likely be used during armed conflicts as part of wider, conventional or nuclear campaigns. An example would be the 2008 South Ossetia War. Russia has been accused of utilising cyber-attacks whilst at the same time conducting a conventional attack against Georgia (Leyden, 2009). Before taking the information too seriously, analysts must consider that Georgia is a very weak state in terms of I.T. (Cooperative Cyber Defence Centre of Excellence, 2008, p. 5-7). What, however, must be taken seriously is not the allegation that Russian intelligence agencies were involved (McMillan, 2009) but the allegation that Russian non-state actors were involved (Wentworth, 2008).

The analysis provided here goes some way towards showing that a kinetic cyber-attack is yet to appear, as has been demonstrated with references to such cases as Stuxnet and Estonia which have not been anywhere near as dangerous as the scenarios dreamt up by various groups. To avoid armed conflicts, the US in particular has to ensure that its software and systems developers are creating platforms that perform to the highest standard without vulnerabilities, and by educating employees who are making use of I.T. By closing off the access point, there will be no way in for foreign agents to get into systems. The danger for the US (and NATO) is to declare a 'war on cyber-attacks', like it did on terror. The US and at least other major I.T. powers should agree on a kind of convention, perhaps like the Chemical Weapons Convention (Geers, 2010), thereby clearly defining what is attack and what is espionage. Cyber-attacks in themselves will not cause conflicts, as I do not believe that there is any state which would conduct a war merely making use of cyber-attacks. Any first strike will always be conventional or nuclear, but cyber-attacks will accompany such strikes, most likely in the same way that Israel used information attacks to blind the Syrian air defence system (Aviation Week, 2007) on its attack against an alleged Nuclear reactor (Heinrich, 2010). The 21$^{st}$ century will see a plethora of cyber-attacks, with the vast majority merely constituting espionage. Those that are not espionage will be attacks utilised to pave the way for various forms of conventional attacks. The Internet as an asymmetric kinetic weapon delivery system remains unproven, and the risk of cyber-adventurism by a state is much lower than is being portrayed by many different institutions and stakeholders.

## Bibliography:

Advanced Systems Group – White Paper., 2010. The Case for a New Approach to Network Security. [online] The Advanced Systems Group. Available at: <http://www.virtual.com/whitepapers/asg-network-security-whitepaper.pdf> [Accessed 30 November 2012].

Arquilla, John, 2012. Cyber War Is Already Upon Us, Foreign Policy [online] March. Available at: <http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us?page=0,0http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us?page=0,0>
[Accessed 28 November 2012].

BBC, 2005. German Admits Creating Sasser, BBC, [online] 5 July. Available at:
<http://news.bbc.co.uk/1/hi/technology/4649361.stm>
[Accessed 01 December 2012].

Boyd, Clark., 2008. Profile: Gary McKinnon, BBC [online] 30 July. Available at:
<http://news.bbc.co.uk/1/hi/technology/4715612.stm>
[Accessed 27 November 2012].

Burt, Jeffery, 2012. Kaspersky: Flame and Similar Malware Pose Worldwide Risk, eWeek, [online] 7 June. Available at: < http://www.eweek.com/c/a/Security/Kaspersky-Flame-and-Similar-Malware-Pose-Worldwide-Risk-167793/> [Accessed 01 December 2012].

Cole, A., Gorman, S., Dreazen, Y. J., 2009. Insurgents Hack US Drones, The Wall Street Journal, [online] 19 December. Available at: <http://online.wsj.com/article/SB126102247889095011.html>
[Accessed 29 November 2012].

Cooperative Cyber Defence Centre of Excellence., 2008. Cyber Attacks Against Georgia. [online] Cooperative Cyber Defence Centre of Excellence. Available at: <http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf> [Accessed 30 November 2012].

Cyber officials: Chinese hackers attack 'anything and everything', FCW, [online] 13 February. Available at: <http://fcw.com/articles/2007/02/13/cyber-officials-chinese-hackers-attack-anything-and-everything.aspx?sc_lang=en> [Accessed 01 December 2012].

Dunn, Ashley, 1999. Battle Spilling Over Onto Internet, LA Times, [online] 3 April. Available at:
<http://articles.latimes.com/1999/apr/03/news/mn-23851> [Accessed 01 December 2012].

Dartmouth, 2012. Gary McGraw: Cyber War, Cyber Peace, Stones, and Glass Houses . Available at: <http://www.youtube.com/watch?v=LCULzMa7iqs> [Accessed 30 November 2012].

Denning, Dorothy E., 2003. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. [online] The Information Warfare Site. Available at: <http://www.iwar.org.uk/cyberterror/resources/denning.htm> [Accessed 30 November 2012].

DoD News Briefing – Secretary Rumsfeld and General Myers. US Department of Defense. [online] Available at: <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636> [Accessed 10 December 2012 ].

Fault Lines – Cyberwar. Al Jazeera. [online video] Available at: <http://www.aljazeera.com/programmes/faultlines/2010/04/2010421152728872905.html > [Accessed 30 November 2012 ].

F-Secure, 2010. Stuxnet Questions and Answers. [online] F-Secure. Available at: <http://www.f-secure.com/weblog/archives/00002040.html> [Accessed 30 November 2012].

F-Secure, 2011. Computer Invaders: The 25 Most Infamous PC Viruses of All Time. [online] F-Secure. Available at: < http://safeandsavvy.f-secure.com/2011/03/21/25-infamous-viruse/l> [Accessed 30 November 2012].

Fulghum, David A., 2007. Why Syria's Air Defences Failed To Detect Israelis, Aviation Week [online] 3 October. Available at: <http://www.aviationweek.com/Blogs.aspx?plckBlogId=Blog:27ec4a53-dcc8-42d0bd3a01329aef79a7&plckController=Blog&plckScript=blogScript&plckElementId=blogDest&plckBlogPage=BlogViewPost&plckPostId=Blog%253a27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%253a2710d024-5eda-416c-b117-ae6d649146cd>[Accessed 27 November 2012].

Geers, Kenneth. Cyber Weapons Convention. Computer Law and Security Review, 2010, Volume 26, pp. 547-551

Glaser, Charles L., Deterrence of Cyber Attacks and US National Security. The George Washington Cyber Security Policy and Research Institute, 2011. Available at: http://www.cspri.seas.gwu.edu/Seminar%20Abstracts%20and%20Papers/20115%20Cyber%20Deterrence%20and%20Security%20Glaser.pdf

Goldstein, Guy Philippe How cyberattacks threaten world peace. TED. [online video] Available at: <http://www.ted.com/talks/guy_philippe_goldstein_how_cyberattacks_threaten_real_world_peace.htl> [Accessed 01 December 2012 ].

Gorman, S. & Barnes, E.J., 2011. Cyber Combat: Act of War, The Wall Street Journal, [online] 30 May. Available at: <http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html> [Accessed 25 November 2012].

Hathaway, O.A., Crootof, R., Levitz P., Nix H., Nowlan, A., Purdue, W., Spiegel, J., The Law of Cyber Attacks California Law Review, 2010, Volume 100, pp. 817-886

Heinrich, Mark, 2010. IAEA suspects Syrian nuclear activity at bombed site, Reuters [online] 18 February. Available at: <http://www.reuters.com/article/2010/02/18/us-nuclear-syria-iaea-idUSTRE61H66320100218> [Accessed 28 November 2012].

Internet World Stats, 2012. Top 50 Countries With The Highest Penetration Rate. [online] Internet World Stats. Available at: <http://www.internetworldstats.com/top25.htm> [Accessed 30 November 2012].

Kaspersky, 2011. The Threats of the Age of Cyber Warfare. Available at: <http://www.youtube.com/watch?v=Qsp9SJiCX_I> [Accessed 30 November 2012]

Khan, Huma, 2011. Cyber Attack on U.S. Electric Grid 'Gravest Short Term Threat' to National Security, Lawmakers Say, ABC News [online] 31 May. Available at: <http://abcnews.go.com/blogs/politics/2011/05/cyber-attack-on-us-electric-grid-gravest-short-term-threat-to-national-security-lawmakers-say/>
[Accessed 28 November 2012].

Larsen, Gregory N., & Wheeler, David A., 2003. Techniques for Cyber Attack Atribution. [e-book] Institute for Defense Analyses [Accessed 30 November 2012].

Leyden, John, 2009. Russian spy agencies linked to Georgian cyber-attacks, The Register, [online] 23 March. Available at: <http://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/>
[Accessed 01 December 2012].

Libicki, Martin C. The Specter of Non-Obvious Warfare. Strategic Studies Quarterly, Fall 2012, pp.88-101

Lin, Herbert. Why Computer Scientists Should Care About Cyber Conflict and U.S. National Security Policy. Communications of the ACM, 2010, Volume 55, No. 6, pp. 41-43

Lynn, William J. Defending A New Domain. Foreign Affairs, May 2011, Volume 89, No.5, pp.97-108

McMillan, Robert, 2009. Report Links Russian Intelligence to Cyber Attacks, IT World [online] 20 March. Available at: < http://www.itworld.com/security/64751/report-links-russian-intelligence-cyber-attacks>
[Accessed 28 November 2012].

Meserve, Jeanne, 2007. Official: International hackers going after U.S. networks , CNN, [online] 19 October. Available at: <http://edition.cnn.com/2007/US/10/19/cyber.threats/index.html>
[Accessed 01 December 2012].

Morozov, Evgeny 2010. More on DdoS as Civil Disobedience, Foreign Policy [online] 14 December. Available at: <http://neteffect.foreignpolicy.com/>
[Accessed 28 November 2012].

Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., Brumley, D., GPS Software Attacks. Electric and Computer Engineering at Carnegie Mellon University, 2012. Available at: <http://users.ece.cmu.edu/~dbrumley/courses/18487-f12/readings/Nov28_GPS.pdf>

Parliament, 2008. Judgments – Mckinnon V Government of The United States of America and Another. [online] Parliament. Available at: <http://www.publications.parliament.uk/pa/ld200708/ldjudgmt/jd080730/mckinn-1.htm>
[Accessed 30 November 2012].

Patrikakis, C., Masikos, M., Zouraki, O., Distributed Denial of Service Attacks. The Internet Protocol Journal, Volume 4, No.7. Available at: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html

President of the United States of America., 2011. International Strategy For Cyberspace. [online] The White House. Available at: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>
[Accessed 30 November 2012].

Rid, T & McBurney, P., Cyber Weapons. The RUSI Journal, 2010, Volume 157, No. 1, pp. 6-13

Sanger, David E., 2012. Obama Order Sped Up Wave of Cyberattacks Against Iran, New York Times, [online] 1 June. Available at: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=1&>[Accessed 01 December 2012].

T. Chen and J. M. Robert, The evolution of viruses and worms: Statistical methods in computer security, W. Chen (Editor), Marcel Dekker, 2004.

Tabansky, Lior. Basic Concepts In Cyber Warfare. Military and Strategic Affairs, May 2011, Volume 3, No.1, pp.75-94

Traynor, Ian, 2007. Russia accused of unleashing cyberwar to disable Estonia, The Guardian [online] 7 May. Available at: <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia> [Accessed 28 November 2012].

Wentworth, Travis, 2008. You've Got Malice, Newsweek [online] 22 August. Available at: <http://www.thedailybeast.com/newsweek/2008/08/22/you-ve-got-malice.html >
[Accessed 28 November 2012].

—

*Written by: Asim Rizvanovic*
*Written at: Loughborough University*
*Written for: Dr. Rob Dover*
*Date written: December 2012*