IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 22, Issue 9, Ver. 15 (September. 2017) PP 01-06
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Protecting Australia against Cyberterrorism

Dr. Marcia R Pinheiro
drmarciapinheiro@gmail.com
IICSE University DE, USA

ABSTRACT: We talk about how to best protect Australia against cyberterrorist attacks of the type in which the offenders use a computer to attack or in which the offenders attack computers. Our concern is phenomena like Stuxnet and Ransomware, but also any attack that has not yet happened, as for our official records, so say hacking of satellite and use of its allowances to burn people alive to death. We talk about the basics, which could be the advice of FireEye, and we talk about the sophisticated, which could be what is not yet printed. We worry about actions that could be considered part of the intelligence system, so things that demand detailed study of the past and systemic plus organised collection of data in the present. We do not talk about how to deal with Acts of War: Only about how to protect our systems to best so that we do not get those happening via computer or from a computer.

Keywords: Intelligence, IT, cyberwar, government, Australia

Date of Submission: 18-09-2017 Date of acceptance: 27-09-2017

I. INTRODUCTION

We must share world references (Pinheiro, 2013) to be able to progress together into our discussion (Citizendium, 2013):

1. Defensive counterintelligence: Defensive analysis is the practice of looking for vulnerabilities in one's own organization, and, with due regard for risk versus benefit, closing the discovered holes.
2. Offensive Counterespionage is the set of techniques that, at a minimum, neutralizes discovered FIS personnel and arrests them or, in the case of diplomats, expels them by declaring them persona non grata. Beyond that minimum, it exploits FIS personnel to gain intelligence for one's own side, or actively manipulates the FIS personnel to damage the hostile FIS organization.
3. Counterintelligence Force Protection Source Operations (CFSO) are human source operations, conducted abroad that are intended to fill the existing gap in national level coverage in protecting a field station or force from terrorism and espionage.

The 3rd item is our Collective Counterintelligence (CI): Defensive intelligence is DI, and, offensive intelligence, OI. Having established the world references, we must tell what we discuss, and that is then the topic of our next paragraph.

We talk about infrastructure and cyberterrorism, and therefore about Stuxnet (Zetter, 2014) and DDoS attacks (Armerding, 2016). We should worry about hackers entering our satellites and attacking us through them (Shachtman, 2008) since (Daily Mail Reporter, 2013) at most (Broder, 2016) 2002 (National Space Society, 2016), when researchers from a famous laboratory put a laser transmitter in a satellite (Rubenchik et al, 2009): At most then we should have gotten scared. Worrying about that is part of DI because we do not wait for the news: We guess thinking instead. We need to be prepared for crimes against our machines: automated cars (Mudio, 2016), notebooks, satellite TV (Wong, 2017), telephone, and so on. We also need to be prepared to be attacked inside of our bodies (usa-anti-communist.com, 2010). If we say Information Technology (IT), we assume the aggressor uses an IT tool, say the Internet, when attacking. It is possible to have computers sending signs to computers, and the last one in the series detonating a bomb, perhaps like Mission Impossible (Movieclips, 2016): Just pressing a button causes a catastrophe. When having a Virtual Private Network (VPN) available to them, the aggressor may simulate that they are in Korea (Strouvali, 2015) and attack the supercomputers in Australia in the middle of a major calculation. The government may investigate the incident, blame Korea, and start a war. We discuss that in the next paragraph.

The United States (US) was blamed for the attack on the Iranian nuclear facilities (Farwell and Rohozinski , 2011; Whigham , 2016) and Korea was blamed for the attack on Sony (Altman, 2014). Yet, all

might resume to someone planning all to have those countries appearing as actors, like the perpetrator could be in Brazil, and make use of the VPN system to simulate that they are in Korea instead. We must think about all possibilities: What could the opponent be thinking of doing if what we know to be available to them appeared in their minds as a weapon to do harm? If someone succeeded in stopping the cooling of the nuclear facilities in Japan, all ten units (Hasegawa, 2014), before the first tsunami that hit their plants gets them, and their stop also included shutting down alarm systems, so say if all were connected to computers and the computers were connected to the Internet or the person had an operative doing all via their computers, the results could be a major catastrophe. And why would the evil mind not think like that? DI is definitely not connected to passive attitude: We need to go beyond what is usually imagined. After analysing possible future moves of the adversary, we draw deterrence strategies (Irwin, 2017) or, if avoidance is not possible, we minimize impact (Florence, 2013). We study procedures that may guarantee the safety of the governmental machines: We want to lower down the chances that such things happen. For that, we consult the CI (BastiaensUlrike et al, 2007). In the next paragraph, we tell how this paper is structured and what we do not discuss.

In the section Development, we describe the problem better, and present arguments in favor of our suggestions and against some current procedures even in terms of enforcement. In the section Conclusion, we present our recommendations, and our summary of results. We still talk about limitations in the current study and future work. We do whatever we can to equip the reader with information that is enough for them to inspire themselves and work on good threads of intelligence in order to improve their organizational defensive power by much. We will not discuss how countries should be dealing with possible Acts of War (attacks of other countries to their infrastructure via computers and alike): We talk about how to protect Australia, so that those attacks do not happen instead. In the next paragraph, we give hints on what our suggestions are plus a flash sight of our backstage for this piece.

Our problem is how to stop attacks that come via computer or target computers or at least how to stop a meaningful number and amount of variety of those. Our conclusions are that we should focus on processes of selection and hiring of Information Technology (IT) professionals, firewall policy, storage policy, distribution of personal computers, portable and external storage devices policy, professional networking policies, institutional relationships with vendors and their support teams, complaint and protest policies, human rights in general, space scrutiny policies, emergency policies for IT, alternative currency policies, emergency policies for financial institutions for situations of terrorism, satellite authorization policies, identification policies for hardware of the type computer, training policies for IT staff, including what is trivial in our basic operational IT policies, internal justice systems, and policies for dealing with Acts of War or what looks like them inside of IT.

II. DEVELOPMENT

One of the worst problems with IT crimes is attribution (Rid and Buchanan, 2015): Even if we get the Internet Protocol (IP) of the perpetrator's computer, we cannot easily determine the author of the attack because the aggressor may have used someone else's machine, and at least sometimes the owner of the machine is unaware of that (Khan, 2016). The author of the attack may still use a fake IP: Several browsers let us use a fake IP address online (Burdette and Unwala (eds), 2016); VPNs may help us get anonymous access to the Internet (Robinson, 2017); Dark Webs help people trade valuables without being noticed (Finklea, 2017). Attribution problems are then connected to anonymous surfing or use of third-party vehicles. We need to now find the context in which attribution problems appear connected to the two types of attack we study. In the next paragraph, we explore ransomware and Infrastructure attacks.

With Ransomware (Rajput, 2017), we need to identify perpetrators instantaneously to stop attacks and recover services. In this case, what remains to the government is only anti-hacking. The own government paid ransom (Bennet and Williams, 2016) instead. That is understandable because hacking is usually considered crime, and therefore if law enforcement agents start practicing anti-hacking, which is the only thing that could stop the offender in time, we are in the situation of legalizing and trivializing crime of the same type as the crime we claim to be combatting. Here is the paradox: Agents could perhaps become ethical hackers (Oxford University Press, 2017). Alazab (2017) calls those white hats. The issue is that the government cannot support or incite illegal actions. Similar issues appear in connection with intelligence agencies: If they exist, the government signs under the crimes of a few (Hagopian, 2014; Ingersoll, 2013), and those work for it. That makes governmental agents look like terrorists, and the own government like a terrorist organization (Nelson, n.d.; Meyer, 2012). Maybe they are a necessity (Darling et al, 2007). We choose to ignore anti-hacking: We produce money that is good only to pay ransoms, marked money, and then chase it. We can also invest in the area of infrastructure and hardware tracking of perpetrators. In this case, the investment should be in Engineering: Each machine could emit special identifying marks that nobody knows about apart from manufacturers. Through such signs, enforcement can quickly reach the perpetrator. We can pass directives to all organizations that deal with money, so that ransomware money is marked even when it comes in the shape of a credit card: A few codes, such as, *ask if that is OK*, and the banks start terrorist attack procedures (Uniwersytet

Medyczny, 2016). With attacks of the type Stuxnet (Zetter, 2014), it seems that the perpetrator goes locally and infects the SCADA (Robles et al, 2008) system via USB stick that carries the vector. In this case, the best solution is guaranteeing that no USB enters the facilities that be not a fresh, just formatted or unpacked, USB, like the IT support people must have a system that guarantees that only USBs they personally inspected and classified as good enter their system. One possibility would be making sure that everyone gets fresh USBs to use each, and every, day and they deposit their USBs somewhere by the end of the journey. This is good procedures for attacks of the type Stuxnet, but we have to think of attacks in general, so that we talk about firewalls and IT teams in the next paragraph.

A good firewall (Avolio and Avolio Consulting, 1999) is an essential element to stop attacks that are already known, so say Sheur (AVS Technologies, 2016). Having a good firewall is not enough: We need to be able to optimize its use. Putting the right team in charge of IT (Schmitt, 2012) and providing adequate training (Beauchamp et al, 2017) may make an organization excel in IT security: The attacks to Target in 2013 would not have happened if the IT professionals from Target had heard the vendor in time (Westervelt, 2014). When we think about a good IT team, we think of people who would tell us to do at least the basics in security. Certain things are obvious to everyone, such as only allowing people to do the strictly essential in a machine: Nobody needs to access the MS-DOS prompt if all they will do is researching into a specific catalogue at that location (Brown University, 2015). A few more items form the list of the basics in IT, and we should all be aware of those. A good relationship with providers of software and hardware and the support people from those (FireEye and Target are examples (Westervelt, 2014) allied to pertinence to professional networks (Hermanrud I, 2009) that are technical and can be trusted are also what makes the differential between those who excel in security and those who fail so badly that their machines lose trade capability for many days (Telegraph Media Group, 2017; Corderoy, 2017; Lord, 2017).

> … a ransomware attack last year against a Los Angeles hospital system, Hollywood Presbyterian Medical Center (HPMC), allegedly demanded a ransom of $3.4 million. The attack forced the hospital back into the pre-computing era, blocking access to the company's network, email, and crucial patient data for ten days (Lord, 2017).

For attacks on hospitals, and those happen with a certain frequency (Miles et al, 2017), it seems that having mandatory local storage is paramount, so that every employee should be using a notebook that belongs to the company, is dedicated to their sector, and is not a dumb terminal - a machine that allows them to save both locally and non-locally what they did. We have to have emergency systems also in terms of IT. We seem to be behind in all that has to do with safety in this area, yet we do the impossible when it comes to fire (SBS, 2017), theft (McGee, 2014), and even hurricanes (Jackson, 2017). We still need to have common grounds, so, which attacks that we mention are cyberterrorism?

> Cyberterrorism: Unlawful attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives (Grabosky, 2017).

The definition above is not absolute, but we may expect terrorism to connect to politics. It is called terrorism because it causes terror: What should matter is what we feel when we see news about attacks, when we are victims or when we are witnesses. Stuxnet is a political attack even if there are no banners saying so: Attacks to the infrastructure of a Country are direct attacks to that Country's flag, to their sovereignty. Health is also infrastructure… In the same sense that it suffices that the warship of another Country enter the legal boundaries of ours in an unauthorized manner for us to classify the event as an Act of War (United Nations, n.d.), it suffices that the offenders attack infrastructure for us to classify things as terrorism: That certainly intimidates the nation…The store Target is regarded as one of the Australian icons (Murphy, 2016); Levis (LS&CO, 2017), as an American one. Certain icons do become the nation: We see a McDonald's and we think of America; we see Sony and we think of Hollywood (The Movie Insider LLC, 1999), and therefore America. If an ex-employee (Associated Newspapers Ltd, 2015) did all, it could still be terrorism, for plenty of Australians have joined ISIS (Chambers, 2015): They would attack Australian national symbols if that were of the interest of ISIS. The figure of the insider certainly brings non-negligible loss. Just recently, an MI5 dropped the bomb (Disclose.tv, 2017): The British intelligence did give the order to assassinate Diana. In our best belief, an intelligence agent would never release such a token if he were content with what he did. To keep people without voiding the promises they make to their employers, we need to keep them content with what they do, so that companies should have good complaint and protest lines. They should have a system of internal justice that is exemplary. Insiders happy, how do we protect ourselves against satellite attacks? We talk about this in the next paragraph.

An attack coming from a satellite is terrorism because it is perceived as the same as an alien planet attacking ours (Mighty_Emperor, 2012): Maximum panic. Only continuous monitoring of the activities of the satellites that are in space and strict policies of use could avoid that. Many people are unhappy to levels that could make them think of destroying the planet (Beyond Blue Ltd, 2016; Scientific American and Yuhas, 2012), and one of them could manage to take control of a satellite and, through refined processes of Engineering, burn us all to death. The solution is still making our race happy: Enjoying human rights equates to living life well; actually living it. Islam implies violation of human rights, and the international community proved its power to change Islamic places, ran inside of the model of perhaps dictatorship, into democracies from day to night (Pew Research Center, 2005), so that we should invest in guaranteeing, initially by means of rules, the basic human rights of the women who live in Islam. Nobody should be born without rights to exclusivity over their bodies: Bodies mean human life…The human rights declaration, currently exhibited on the United Nations (UN) pages, needs to be fixed to help women connect to those, since a few rights are stated as if they have been granted only to men: articles 10 to 13, 15, 17 to 18, 21 to 23, 25, and 29 (United Nations, 2017). Scientology has a few of its principles associated with the sigmatoid (Pinheiro, 2015) man (Church of Scientology International, 2017), not humans. That has to be fixed: Women must feel equal to men. It is the feeling of uneven treatment that makes plenty of us unhappy to maximum level. It is unlikely that we stop a home-made satellite from cutting our bodies with a laser beam. It is also unlikely that we stop someone from attacking us with their bare hands in a fatal way. It is possible to inspect any legally authorized satellite sent to space before it is in space, however. It is also possible to monitor activities and even surfaces of all those that our instruments can detect in the same way it would be possible to investigate the past of an individual and gather information about past violence against third-parties.

III. CONCLUSION

On the safest end of the IT hazard spectrum, we must invest in selection, training, and standards. We must have storage and independent systems everywhere. Wherever there is the need of using USB sticks or other items of possible criminal penetration, IT professionals should guarantee that the material is picked at the workplace fresh every day and dropped by the end of the shift for maintenance. Every company should have emergency procedures also for when the computer system fails, not only for when there are fires or hurricanes. Firewalls are essential elements of protection. Restrictions in use are not only necessary: They are mandatory. Anti-hacking (OI) probably means crime, so that enforcement cannot invest in that: Instead, they should invest in marked money to pay ransomware, and then quickly trace perpetrators (DI). They could also invest in Engineering and mark incoming traffic, so say machine XDZ789. Finding the machine of the perpetrator does not mean finding them (CI may be needed), but we could also associate the individual's ID with the machine's ID, perhaps in a manner that only the official authority knows. Our internal systems of complaint and justice must do more for our employees than the external ones (DI). The world should declare war against regimens that make some be legally deprived from basic rights, as it is the case with Islam (women are not free). Sole ownership of our bodies is essential: The minimum requisite for human happiness is that our bodies be exclusively ours (DI). Organizations must not use gender-exclusive language, so that they should say human instead of his, man, and others (DI). We should set directives to all organizations that are officially authorized to deal with money, so that they know when the government needs their help and also what to do: An emergency IT plan (DI). Any machine that *lives* in the space should be continuously monitored and inspected in a rigorous way before being put there (DI). We should make sure human kind is happy, so that people do not feel like betraying their organizations, partners, and others; in special, so that they do not feel like destroying them (DI). Recommendations are good, but we must also talk about the concept of cyberterrorism, limitations in our study, and possible future developments. These are the topics of our next paragraph.

Cyberterrorism also comprises of attacks on symbols, so that it is an expression that goes well beyond governmental institutions: Target is probably a symbol for Australia, and McDonald's plus Levis are probably symbols for the US. Many of the cyber terrorist activities can be faced as acts of war, and therefore probably deserve compatible treatment (DI). Certain attacks will never be detected or stopped in time, so that failure is part of the intelligence business. We also need to talk about the limitations and possible developments of this study. We did not talk enough about Acts of War: We talked about how to protect Australia, so that those attacks do not happen instead. Further research is needed to address Possible Acts of War. The issues that most cause concern are attribution, in special equivocated attribution, and the consequences involved. We here studied a very small number of cases and limited information about those. Better results could be obtained from a much bigger sample of real-life cases and a much larger set of details.

REFERENCES

[1]. Alazab M. (2017) PICT 840: Cyber Crime Hacking: motives, methods, and organizations. Available at: http://ilearn.mq.edu.au/pluginfile.php/4663801/mod_resource/content/1/Week 3.pdf.

[2]. Altman A. (2014) Everything We Know About Sony, The Interview and North Korea. Available at: http://time.com/3639275/the-interview-sony-hack-north-korea/.
[3]. Armerding T. (2016) Is Critical Infrastructure the Next DDoS Target? Available at: http://www.csoonline.com/article/3141601/critical-infrastructure/is-critical-infrastructure-the-next-ddos-target.html.
[4]. Associated Newspapers Ltd. (2015) Crippling Sony Hack was the Work of a Disgruntled Former Employee Named Lena who Was Laid off'. Available at: http://www.dailymail.co.uk/news/article-2893509/Security-officials-say-crippling-Sony-hack-inside-job-work-disgruntled-former-employee-named-Lena-laid-off.html.
[5]. Avolio F and Avolio Consulting (1999) Firewalls and Internet Security. The Internet Protocol Journal 2(2). Available from: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-1/ipj-archive/article09186a00800c85ae.html.
[6]. AVS Technologies. (2016) Trends & Statistics for Malware Detected. Available at: http://www.avgthreatlabs.com/en-au/virus-and-malware-information/?_ga=2.29229820.1362416178.1505114873-2081500878.1505114873&utm_expid=34410884-80.xo6PQT6XSWeQhLJ4I6LP5A.0.
[7]. BastiaensUlrike TJ et al (2007) An Approach for the Visual Representation of Business Models that Integrate Web-Based Collective Intelligence into Value Creation. In: On Collective Intelligence, pp. 25–35. Available from: https://link-springer-com.simsrad.net.ocs.mq.edu.au/book/10.1007%2F978-3-642-14481-3.
[8]. Beauchamp MR et al. (2017) The Effectiveness of Teamwork Training on Teamwork Behaviors and Team Performance: A Systematic Review and Meta-Analysis of Controlled Interventions. PloS one. Available from: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0169604.
[9]. Bennet C and Williams KB. (2016) Ransomware Takes Millions, Baffles Law Enforcement. Available at: http://thehill.com/policy/cybersecurity/270097-ransomware-takes-millions-baffles-law-enforcement.
[10]. Beyond Blue Ltd. (2016) Statistics and References. Available at: https://www.beyondblue.org.au/about-us/research-projects/statistics-and-references.
[11]. Broder J. (2016) Why the next Pearl Harbor Could Happen in Space. Available at: http://www.newsweek.com/2016/05/13/china-us-space-wars-455284.html.
[12]. Brown University. (2015) Acceptable Use Policy. Available at: https://it.brown.edu/computing-policies/acceptable-use-policy.
[13]. Chambers G. (2015) Revealed: Full List of Aussie Jihadis Fighting with ISIS in Syria and Iraq. Available at: http://www.dailytelegraph.com.au/news/nsw/revealed-full-list-of-aussie-jihadis-fighting-with-isis-in-syria-and-iraq/news-story/bc2b29a864c20f5affffef8e8d3a368f.
[14]. Church of Scientology International. (2017) Scientology Beliefs. Available at: http://www.scientology-detroit.org/local/detroit/scientology-beliefs.html.
[15]. Citizendium . (2013) Counterintelligence. Available at: http://en.citizendium.org/wiki/Counterintelligence.
[16]. Corderoy J. (2017) Massive Cyber AttackCcreates Chaos around the World. Available at: http://www.news.com.au/technology/online/hacking/massive-cyber-attack-creates-chaos-around-the-world/news-story/b248da44b753489a3f207dfee2ce78a9.
[17]. Daily Mail Reporter. (2013) King of Spy Satellites: Huge 68ft Device that will Record Zoom-able HD Video of 40% of Earth's the Surface SIMULTANEOUSLY. Available at: http://www.dailymail.co.uk/sciencetech/article-2521162/Pentagon-designing-satellite-spy-40-Earth-once.html.
[18]. Darling AB et al. (2007) The Central Intelligence Agency: An Instrument of Government, to 1950. Penn State Press. Available from: https://books.google.com.au/books?id=gJO1MQrsUtAC&dq=why+one+needs+intelligence+agencies&source=gbs_navlinks_s.
[19]. Disclose.tv. (2017) Retired MI5 Agent Confesses: I Assassinated Princess Diana. Available at: http://www.disclose.tv/news/retired_mi5_agent_confesses_i_assassinated_princess_diana/139396.
[20]. Finklea K. (2017) Dark Web. Available at: https://fas.org/sgp/crs/misc/R44101.pdf.
[21]. Florence A. (2013) Risk Management. Available at: http://www.asq509.org/ht/a/GetDocumentAction/i/79426.
[22]. Grabosky P. (2017) Cyberterrorism, Cybercrime and the State. Available at: http://ilearn.mq.edu.au/pluginfile.php/4663825/mod_resource/content/1/Slides.pdf.
[23]. Hagopian J (2014) Getting Away with Murder: Immunity of US Intelligence from Criminal Prosecution. Global Research June 12. Available from: http://www.globalresearch.ca/getting-away-with-murder-immunity-of-the-us-intelligence-from-criminal-prosecution/5386827.
[24]. Hermanrud I. (2009) Professional Networks and Knowledge Sharing - the Role of ICT Use a Comparative Study. Available at: https://www2.warwick.ac.uk/fac/soc/wbs/conf/olkc/archive/olkc4/papers/1aingehermanrud.pdf.
[25]. Ingersoll G. (2013) CIA Agents Sleep Around All The Time, Says Ex-Spook. Available at: https://www.businessinsider.com.au/secret-agents-have-sex-all-the-time-2013-2?r=US&IR=T.
[26]. Irwin A (2017) Week 2 Knowing Ourselves and Knowing our Enemies. Sydney: Macquarie University. Available from: http://ilearn.mq.edu.au/pluginfile.php/4583694/mod_resource/content/11/PICT849_Lecture 2_S2_2016_Knowing Ourselves and Knowing our Enemies.pdf.
[27]. Jackson T. (2017) CHP Installation Keeps Hospital Running During Hurricane Harvey. Available at: https://energy.gov/eere/amo/articles/chp-installation-keeps-hospital-running-during-hurricane-harvey.
[28]. James P. Farwell and Rohozinski R (2011) Stuxnet and the Future of Cyber War. Survival 53(1): 23--40. Available from: http://www-tandfonline-com.simsrad.net.ocs.mq.edu.au/doi/pdf/10.1080/00396338.2011.555586?needAccess=true.
[29]. Khan MA (2016) Cyber Crimes: A Fresh Look. International Journal of Management and Social Sciences Research (IJMSSR) 5(6): 52–57. Available from: http://www.irjcjournals.org/ijmssr/June2016/6.pdf.
[30]. Koichi Hasegawa (2014) The Fukushima Nuclear Accident and Japan's Civil Society: Context, Reactions, and Policy Impacts. International Sociology 29(4): 283–301. Available from: http://journals.sagepub.com.simsrad.net.ocs.mq.edu.au/doi/pdf/10.1177/0268580914536413.
[31]. Lord N. (2017) A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of all Time. Available at: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.
[32]. LS&CO. (2017) Levi Strauss. Available at: http://www.levistrauss.com/our-story/.
[33]. McGee MK. (2014) Prison Term for ID Theft at Hospital. Available at: https://www.databreachtoday.com/prison-term-for-id-theft-at-hospital-a-7680.
[34]. Meyer P. (2012) The CIA as a Terrorist Organization. Available at: http://www.serendipity.li/cia/cia_terr.html.
[35]. Mighty_Emperor. (2012) Space horror. Available at: http://www.imdb.com/list/ls050193364/.

[36]. Miles J et al. (2017) Queensland Health's Electronic Medical Records System Hit by Very Serious Ransomware Attack. Available at: http://www.couriermail.com.au/news/queensland/queensland-government/queensland-healths-electronic-medical-records-system-hit-by-very-serious-ransomware-attack/news-story/b8c7ee3486c7cd1546fe130499384366.
[37]. Movieclips. (2016) Mission: Impossible - Ghost Protocol (10/10) Movie CLIP - Mission Accomplished (2011) HD. Available at: https://www.youtube.com/watch?v=PhbkMQ89QPM.
[38]. Mudio D. (2016) Self-driving Cars Are Prone to Hacks -- and Automakers Are Barely Talking about It. Available at: https://www.businessinsider.com.au/driverless-cars-hacking-ricks-2016-12?r=US&IR=T.
[39]. Murphy J. (2016) The Drama at Big W and Target Could Make Kmart the last Man Standing. Available at: http://www.news.com.au/finance/business/retail/the-drama-at-big-w-and-target-could-make-kmart-the-last-man-standing/news-story/945e4cb3f07667973ce5b60cf399a6a8.
[40]. National Space Society. (2016) Space Solar Power. Available at: http://www.nss.org/settlement/ssp/.
[41]. Nelson C. (n.d.) The CIA -- a Terrorist Organization. Available at: http://www.informationclearinghouse.info/article17695.htm.
[42]. Oxford University Press. (2017) Ethical Hacker. Available at: https://en.oxforddictionaries.com/definition/ethical_hacker.
[43]. Pew Research Center. (2005) No Title. Available at: http://www.pewforum.org/2005/11/04/islam-and-democracy-iraq-afghanistan-and-pakistan/.
[44]. Pinheiro MR. (2013) Essential Notes. PROz.com Translation Article Knowledgebase. Available at: http://www.proz.com/translation-articles/articles/3748/1/Essential-Notes.
[45]. Pinheiro MR (2015) Words for Science. Indian Journal of Applied Research 5(5): 19–22. Available from: https://www.worldwidejournals.com/ijar/articles.php?val=NjQ0MQ==&b1=853&k=214.
[46]. Rajput TS (2017) Evolving Threat Agents: Ransomware and their Variants. International Journal of Computer Applications 164(7): 28–34. Available from: http://www.ijcaonline.org/archives/volume164/number7/rajput-2017-ijca-913666.pdf.
[47]. Rid T and Buchanan B (2015) Attributing Cyber Attacks. Journal of Strategic Studies 38(1–2). Available from: http://www-tandfonline-com.simsrad.net.ocs.mq.edu.au/doi/abs/10.1080/01402390.2014.977382.
[48]. Robinson SC (2017) What's Your Anonymity Worth? Establishing a Marketplace for the Valuation and Control of Individuals' Anonymity and Personal Data. Available from: https://www.researchgate.net/publication/317304352_What's_Your_Anonymity_Worth_Establishing_a_Marketplace_for_the_Valuation_and_Control_of_Individuals'_Anonymity_and_Personal_Data.
[49]. Robles1 RJ et al. (2008) Vulnerabilities in SCADA and Critical Infrastructure Systems. International Journal of Future Generation Communication and Networking 1(1): 99–104. Available from: http://www.sersc.org/journals/IJFGCN/vol1_no1/papers/14.pdf.
[50]. Rubenchik AM, Parker JM, Beach RJ, et al. (2009) Solar Power Beaming: From Space to Earth. Available at: https://e-reports-ext.llnl.gov/pdf/372187.pdf.
[51]. SBS. (2017) Hospital Fire Safety Doubts Prompt Probe. Available at: http://www.sbs.com.au/news/article/2017/06/30/hospital-fire-safety-doubts-prompt-probe.
[52]. Schmitt N (2012) The Oxford Handbook of Personnel Assessment and Selection. Oxford University Press. Available from: https://books.google.com.au/books?id=HZJpAgAAQBAJ&dq=selection+of+it+professionals+journal+best&source=gbs_navlinks_s.
[53]. Shachtman N. (2008) Pentagon Spy: Terrorists Ready to Launch Satellite Strikes by 2020. Available at: https://www.wired.com/2008/06/the-defense-int/.
[54]. Strouvali S. (2015) How to Change Your IP to any Other Country You Want. Available at: https://securitygladiators.com/change-ip-to-other-country/ .
[55]. Telegraph Media Group. (2017) British Airways Chaos: All Flights Cancelled at Heathrow and Gatwick after Global Computer Failure. Available at: http://www.telegraph.co.uk/news/2017/05/27/british-airways-chaos-computer-systems-crash-across-world-causing/.
[56]. The Movie Insider LLC. (1999) Sony Pictures. Available at: https://www.movieinsider.com/c8/sony-pictures.
[57]. United Nations. (2017) Universal Declaration of Human Rights. Available at: http://www.un.org/en/universal-declaration-human-rights/.
[58]. United Nations. (n.d.) Part II Territorial Sea and Contiguous Zone. Available at: http://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm.
[59]. Uniwersytet Medyczny. (2016) Procedures in Case of Emergency and Terrorist Attack. Wroclaw. Available at: https://www.ed.umed.wroc.pl/sites/default/files/ed/files/PROCEDURE_IN_CASE_OF_EMERGENCY_AND_TERRORIST_ATTACK_wersja_angielska(1).pdf.
[60]. Unwala A and Burdette Z (eds) (2016) Georgetown Journal of International Affairs: International Engagement on Cyber V. Georgetown University Press. Available from: https://books.google.com.au/books?id=j1ARDQAAQBAJ&dq=tor+browser+journal+cyber&source=gbs_navlinks_s.
[61]. usa-anti-communist.com. (2010) Microwave Weapons Used In Directed Energy Weapon Attacks On Individuals & Global Criminal Use Of DEWs. Available at: http://www.usa-anti-communist.com/ard/microwave-weapons.php.
[62]. Westervelt R. (2014) Missed FireEye Alerts Reportedly Warned Of Security Lapse At Target. Available at: http://www.crn.com/news/security/300072031/missed-fireeye-alerts-reportedly-warned-of-security-lapse-at-target.htm.
[63]. Whigham N. (2016) Alex Gibney Film Gives Chilling Insight into the World of State Sponsored Cyber Warfare Unleashed by Stuxnet. Available at: http://www.news.com.au/technology/online/security/alex-gibney-film-gives-chilling-insight-into-the-world-of-state-sponsored-cyber-warfare-unleashed-by-stuxnet/news-story/a7063ae03dcb5cd6ed2a576d6a8ea9dc.
[64]. Wong M. (2017) DirecTV Strikes Back at Hackers. Available at: http://abcnews.go.com/Technology/story?id=98990&page=1.
[65]. Yuhas D and Scientific American. (2012) Do We all Secretly Want the World to End? Available at: http://www.salon.com/2012/12/18/do_we_all_secretly_want_the_world_to_end/.
[66]. Zetter K. (2014) An Unprecedent Look at Stuxnet, the World's First Digital Weapon. Available at: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

Dr. Marcia R Pinheiro. "Protecting Australia against Cyberterrorism." IOSR Journal Of Humanities And Social Science (IOSR-JHSS) , vol. 22, no. 9, 2017, pp. 01–06.