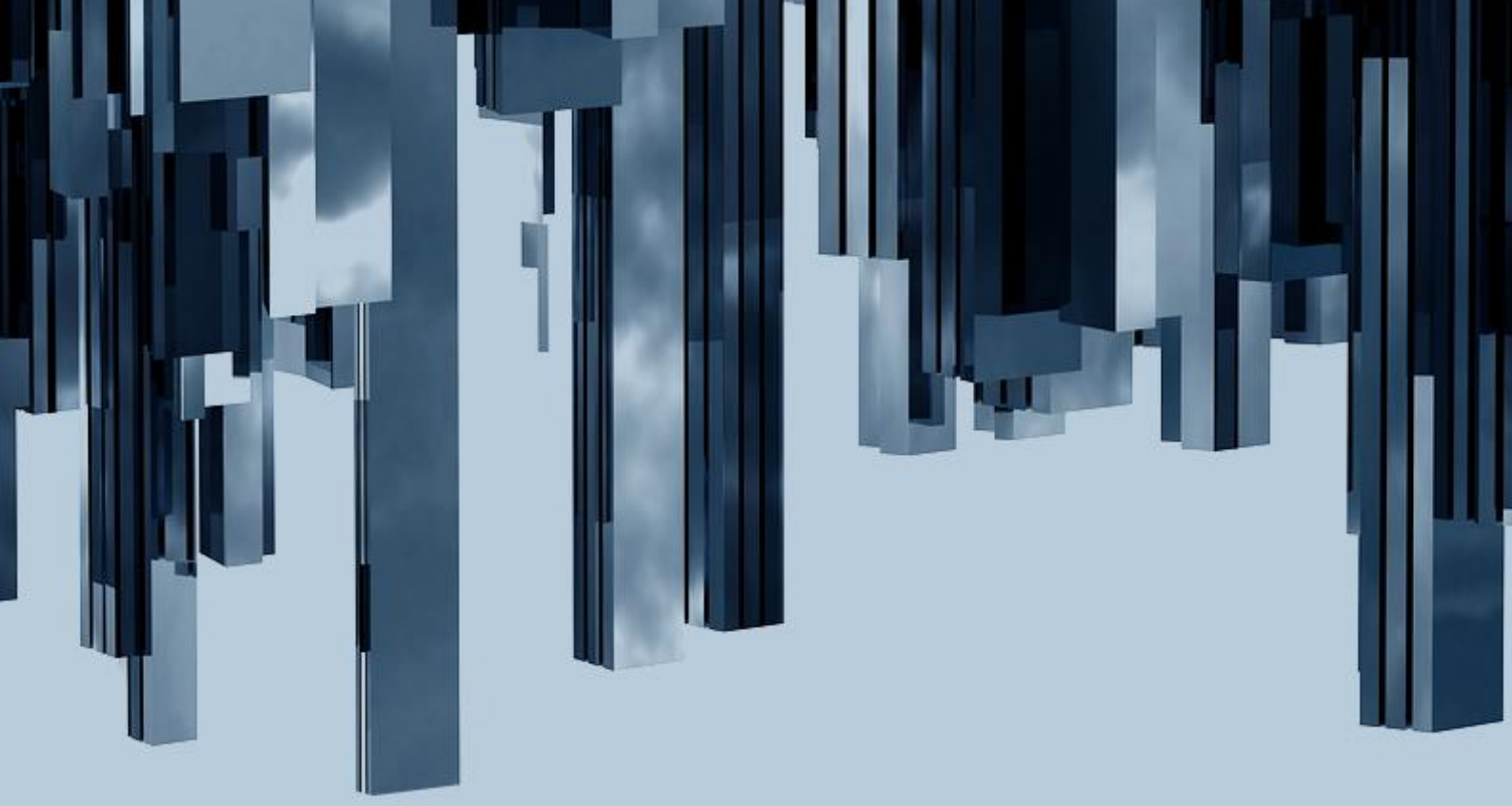

The Greatest Transfer of Wealth in History

How Significant is the Cyber-Espionage Threat?

http://www.henrysevers.com

The Greatest Transfer of Wealth in History: How Significant is the Cyber-Espionage Threat?

Henry Severs

Introduction

This paper presents a brief assessment of cyber-espionage, exploring the increased capacity and enthusiasm to exploit system vulnerabilities to illicitly obtain intellectual property, trade secrets, and competitive advantage. It considers how progressive technologies, tool sharing, and improved technical and social engineering techniques have augmented and transformed modern espionage, making it increasingly easy for malign actors – whether malevolent insiders, foreign intelligence services, or hackers for hire – to steal vast libraries of sensitive information with instant results, zero cost, and relative anonymity.

This investigation is presented through five distinct areas of analysis: After a brief synopsis of the technological and communicative developments which have foster the growth of cyber-espionage, a review of the public, political, and scholarly discourses surrounding cyber-security shall be presented in an effort to establish what we mean by 'cyber-espionage'. This will be followed by a discussion of the many difficulties associated with establishing and recording the true cost of espionage. The ambiguities and cultural disparities found in attempts to accurately attribute offenses to perpetrators shall then be examined, followed by a brief overview of the crucial, but often overlooked, non-technical methods employed in such incidents. In concluding, many of the problems facing policymakers shall be considered, and the need for inter-disciplinary co-operation in formulating a more nuanced, holistic understanding of cyber-security shall be reiterated.

By drawing upon pertinent case studies and applicable theoretical paradigms throughout, gauging the associated assets, exploits, and vulnerabilities involved, I shall demonstrate that not only is cyber-espionage a genuine and escalating threat, but its implications have

far greater consequence for the balance of global power, than traditional military dominance or sensationalist notions of cyber-warfare.

Definitions and Limitations

It is important to recognise this papers limitations, especially approaching an eclectic, multi*disciplinary* field still in its relative infancy[1]. Distinguishing 'cyber-espionage', as considered here, from 'cyber-warfare' is crucial. The former concerns the exploitation of cyberspace and human intelligence as a means of illicitly gathering, collating, and analysing covertly extracted data, the latter focuses on the efficacy of malicious code as a weapon and/or to supplement traditional kinetic warfare[2]. Equally, this paper does not represent a detailed forensic examination of cyber-weapons or DDoS attacks, but instead focuses on the economic, political, and social implications of cyber-espionage. Finally, although many themes presented have wider application, this paper's primary focus is of the infiltration and theft of sensitive data from private companies, research facilities, and government contractors, consequentially one should be cautious when making broader cyber-security generalisations[3].

In order to address the question and circumvent theoretical quandaries debating contentious terms, it is vital to employ solid working definitions from the outset, whilst acknowledging more suitable and descriptive vocabulary may evolve in the future[4]. Throughout, *'the internet'* refers to the "global computer network, providing a variety of information and communication facilities, consisting of interconnected [network of] networks using standardised communication protocols"[5]. Here, *'cyberspace'* is taken as the "total landscape of technology mediated communication" as outlined by Stevens[6]. It takes Rid's[7] definition of '*cyber-espionage'* as "attempt[s] to penetrate an adversarial system for purposes of extracting sensitive or protected information… either *social* or *technical* in nature". It utilises Berners-Lee's description of *'W3'* as "the universe of network-accessible information, resources and users on the Internet...using Hypertext-Transfer-Protocol"[8].

[1] Shipman, (1997)
[2] Clarke, (2010)
[3] NCIX, (2011:i-iii)
[4] Shipman, (1997:16)
[5] ODO, (2012); Gralla, (2007:7)
[6] Stevens & Neumann, (2009:10)
[7] Hoffman, (2006:40)
[8] Berners-Lee, (2001)

Globalisation and Late-modernity

The exponential rise of information based economies, concomitant to the universal ascension of the internet and other advanced computer mediated communications (CMC), are unprecedented modern phenomena. Alongside other pervasive expressions of late-modernity and globalisation, they will likely come to epitomise this phase of human history as the enlightenment and industrial revolution have previous centuries[9]. Huge advancements in the speed, volume, and accessibility of information, as well as the systems and virtual architecture that constitute and sustain cyberspace[10], have transformed the way we communicate, work, trade, innovate, research, develop, and store information in our increasingly 'glocal' world[11].

The rapid growth experienced by China and India especially, but also Vietnam, Russia, Indonesia, and Brazil, have seen new global players emerge, which have begun to challenge the hegemonic dominance of the West[12]. Technological advancements in CMC saw internet penetration and W3 usage increase by 556% in 12 years; from 360 million in 2000, to 2.4 billion in 2012[13]. By 2016 the world population is expected to reach 7.3 billion, with internet facing mobile devices topping 10 billion[14]. Whilst cyberspace has cultivated and nurtured innovation, productivity, efficiency, and transnational co-operation, it has simultaneously exposed vulnerabilities and revealed new threats, due to its open nature and our increased reliance upon it[15]. It is no surprise malevolent actors have also enthusiastically exploited the internet to infiltrate and extract information from opponents at immense speeds and on enormous scales, underscoring the changing nature of espionage and the increasing redundancy of traditional counter-measures[16].

Discourse and Rhetoric

Aside from detailed and rapidly evolving computer science analysis, a cursory examination of the current literature reveals a tendency to focus on government-centric paradigms, offensive strategies, and warfare models of cyber security[17]. These themes have reinforced

[9] Bauman, (2000); Millard, (2011)
[10] IWS, (2012); Knight, (2003:15); Ahlgren,.(2005); Edensor, (2001)
[11] Roudometof, (2005); Appadurai, (1990); Giddens, (1991)
[12] Wolfowitz *in* Alexander, (2012); Baumann, (2000)
[13] IWS, (2012)
[14] Alexander, (2012)
[15] *ibid.*
[16] Foryst, (2010)
[17] Rid, (2012:5-6)

sensationalist public discourses, and apocalyptic moral panics concerning cyber attacks[18]. Leon Panetta's almost Nostradamian predictions of a pending "cyber Pearl Harbour", and Vanity Fair's equally inane and rather crass analogy of the Stuxnet virus as the "Hiroshima of cyber-war", are perhaps most infamous examples of this[19]. The end-of-days rhetoric propagated by Clarke[20], in which planes fall from the skies, trains derail, critical infrastructure fails, nuclear reactors meltdown, and military defences crumble, appears to have become an recurrent narrative in both the wings of Washington and the corridors of Whitehall.

In an attempt to substitute the sensational for the rational, and replace the speculative with the empirical, scholars and policy makers alike should be mindful that *all* known instances of politically motivated cyber-attack are essentially advanced versions of three activities; sabotage, subversion, and, of course, espionage[21]. Whilst these actions are certainly as ancient as warfare, they do not constitute an act of war in the classic Clausewitzian[22] sense, as the three constitutive elements of war are not present: *violence* and potential lethality of the act, the *instrumental* imposition of will, and a *political impetus* and thus discernible culpability. Indeed the majority of oft-cited incidents of 'cyber-war' have, in fact, been cases of espionage, and although the level of technical expertise and complexity may be high, espionage by its very nature is not explicitly instrumental, let alone violent[23]. Cyber-espionage amounts to the clandestine gathering of information that may *subsequently* help establish better instruments of war, inform tactical decisions (or as is increasingly the case) enhance commercial advantage, secure material assets, resources, and business dominance. Given there is no direct linear relationship between computer keystrokes and physical violence, 'cyber-war' is unlikely to replace kinetic military tactics anytime soon[24]. However, when considering espionage, cyber methods not only supplement, but now surpass, traditional methods as the primary tactic of infiltration and data exfilitration, begging the question; at what point should one drop the 'cyber' prefix, and simply talk of 'espionage'?

[18] Cohen, (1972)
[19] Panetta, (2012); Gross, (2011)
[20] Clarke, (2010)
[21] Rid, (2012)
[22] Clausewitz, (1832)
[23] Rid, (2012)
[24] Rid, (2012)

Discovered in 2012, *Flame* is an important example of "a complete attack toolkit designed for general cyber-espionage purposes"[25] and is probably "the most complex malware ever found"[26]. Flame infected approximately 1,000 specific machines including governmental organisations, educational and research institutions, and private computers across the Middle East[27]. Partly written in Lua script with linked C++ code, the dropper allowed for other attack modules to be loaded after initial infection[28]. An atypically large program at 20 megabytes, Flame utilised five encryption methods and an SQLite database to store information[29]. The injection vector was covert and the malware itself sophisticated, in the sense it ascertained a machine's antivirus software, and customised its behaviour accordingly to reduce detection. It altered filename extensions and protected memory pages, even including a remote 'kill' function to purge itself if identified[30]. Flame also installed a fake audio driver which was used to maintain persistent control over the compromised system[31]. Due to the complex, multifaceted composition of the malware (ostensibly built specifically to attack primarily Iranian targets), it is likely a "nation-state sponsored the research"[32], most commentators have indicated Israeli involvement[33].

Inconsistency, Inaccuracy, and Inaction

Gauging the cost of cyber-espionage, to consumers, companies, and/or governments, has been hugely controversial[34]. How representative estimates are, when compiled by profit-motivated software security companies, should be bore in mind here[35]. Symantec[36] place the cost of intellectual property theft to the U.S. at $250 billion a year, with cybercrime at a further $114 billion annually, or $388 billion inclusive of downtime[37]. McAfee[38] estimated global remediation costs to be a staggering $1 trillion per annum, however this is heavily contested, even by those academics McAfee cite[39]. Detica and the Cabinet Office[40] report the cost of cybercrime to UK to be £27 billion in 2012, of which £16.8 billion amounts to

[25] Albanesius, (2012)
[26] CrySyS Lab, (2012)
[27] Zetter, (2012)
[28] Gostev, (2012); Kindlund, (2012)
[29] CrySyS Lab, (2012)
[30] *ibid.*
[31] Kindlund, (2012)
[32] Lee, (2012)
[33] Erdbrink, (2012)
[34] Maass & Rajagopalan, (2011)
[35] NCIX, (2011:3)
[36] Symnatec Corp. (2012)
[37] Alexander, (2012)
[38] McAffe Inc. (2012)
[39] Maass & Rajagopalan, (2011)
[40] Detica, (2012)

intellectual property theft and industrial espionage. The Data Breach Investigations Report (DBIR)[41] investigated 855 incidents of industrial and corporate systems penetration, recording 174 million compromised records across the US, UK, Holland, Ireland and Australia in 2012. Recently MI5 made the unprecedented move of issuing 300 warning letters to UK business leaders highlighting the risk of "electronic espionage" from "Chinese…organisations"[42]. Indeed according to Jonathan Evans, MI5 Director-General, an "astonishing[ly]" high level of cyber-espionage targets Western nations on an "industrial scale"[43]. These remarks echo General Keith Alexander, NSA Director, who claims cyber-espionage amounts to "the greatest transfer of wealth in history"[44].

Yet despite enormous losses being cited and stark warnings being issued, the *true* extent of cyber-espionage is not fully known and may ultimately be incalculable[45]. The difficulties in precise estimations are many, including but not limited to: *Companies not reporting or publicising losses;* for fear of brand and/or reputation damage, company devaluation, loss of public confidence and sales. *Inconsistency in cost calculations;* does one just include the cost of research and development? Or projected future earnings? Anticipatory costs such as antivirus software, insurance, penetration testing etc.? Consequential direct and indirect expenditures? Responsive costs such as compensation, fines, or remediation?. *Inability to ascribe economic value to certain information*, such as; minutes from meetings, business-to-business correspondence, marketing strategies, or transitory value data. *Apathetic or indifferent reaction to attacks*; companies may misunderstand, respond slowly, or be simply naive to the severity and immediacy the threat poses to their business[46].

Often organisations are unaware or unconcerned their systems have been compromised – of the 855 incidents investigated by the DBIR, 92% did not discover their breach until an external party informed them[47]. One illustration of such indifference is articulated by Brian Shields, former ICT Security Advisor at Nortel Systems, who realised in 2004 that passwords of senior executives had been compromised[48]. Tracing the originating IP address to Shanghai, Shields requested an investigation, yet beyond changing passwords

[41] Verizon, (2012)
[42] Rawnsley, (2011)
[43] Evans, (2012)
[44] Alexander, (2012)
[45] Clarke, (2011)
[46] Faber, (2012); NCIX (2011:2-4)
[47] Verizon, (2012:51)
[48] Gorman, (2012)

no action was taken[49]. In 2008, recurrent background data exchanges with a Beijing server was again detected, unearthing a major eight year data exfiltration stretching back to 2000[50]. Shields wrote a 14 page letter to Nortel's Board of Directors, warning; "the Chinese are still in your system…steal[ing] technologies", and "not [to] trust the security of any [digital] information", as "sales, costing, business strategy, research and development" were being routinely monitored and compromised[51]. Nortel, once valued at $250 billion, went bankrupt the following year in 2009[52].

Over the same 2000-2009 period Nortel's primary competitor, Huawei Technologies, headquartered in Shenzhen China, and founded by ex-military technologist Ren Zhengfei, saw accelerated growth[53]. The year following Nortel's bankruptcy, Huawei, who began internationally trading the year of Nortel's original breach, declared record profits of $3.64 billion[54]. The U.S. House of Representatives Select Committee issued a warning regarding Huawei, both in terms of their business practices and their monopoly of the communication technologies industry[55]. Today Huawei supply 45 of the world's 50 largest telecommunications operators, yet whether Nortel's long-term compromise and eventual collapse is linked to Huawei's extraordinary success remains contentious[56]. Former Nortel CEO Mike Zafirovski maintains those "who looked at [the hacking] did not believe it was a real issue"[57]. The concept of 'groupthink' may have import here – where boardroom conformity to the prototypical collective world-view can bypass critical evaluation, condemning criticism, and rationalising (in)action[58].

Even if decisive action is taken to mitigate losses, often breaches can be concealed from regulators, employees, the public, even shareholders and senior executives[59]. In 2009 hackers pilfered sensitive information regarding Coca-Cola's $2.4 billion attempted takeover of Huiyuan Juice Group, tipped to be the largest foreign acquisition of a Chinese company

[49] Faber, (2012)
[50] *ibid.*
[51] *ibid.*
[52] *ibid.*
[53] Anuradha, (2011)
[54] Boomberg, (2011)
[55] Rogers et al.(2012)
[56] Vance, (2011)
[57] Gorman, (2012:28)
[58] Janis, (1972)
[59] Elgin *et al.* (2012)

in history[60]. Coca-Cola never publicly disclosed the breach, the nature of the attack, or why the Huiyuan deal collapsed three days later[61]. This culture of silence is by no means unique to Coca-Cola, only often later divulged by internal whistle-blowers. Following the theft of sensitive archives, BG Group did not go public[62], neither did steel maker ArcelorMittal after cyber attacks targeted Chinese acquisitions executives, nor did Chesapeake Energy when information relating to their tenure of gas leases was extracted[63]. Indeed, transient or temporal information regarding high-stake business transactions, mergers, and acquisitions has become highly prized and increasingly targeted. A week prior to the Rumaila Iraqi oilfield going to auction, ExxonMobil, Total, Fina and others were infiltrated and bidding information compromised[64]. The world's fourth largest oil field, producing 1.33 million barrels per day, was eventually secured in partnership by China National Petroleum Company[65]. The connection of the two remains debatable.

Attribution, Deniability, and Cultural Biases

The majority of sophisticated cyber-espionage attacks suggest Chinese, Russian or Israeli involvement, although actually attributing responsibility for these incidents has proven a recurrently nebulous, and often politically strenuous issue[66]. The intentional global distribution and obscurity of attacks, via numerous proxy servers across multiple countries, has meant competent hackers can enjoy relative anonymity in committing cyber-espionage[67]. Although often framed as an exclusively technical problem, the issue of attribution is far more multifarious[68]. Attempts have been further confounded by the blurring of criminal and political acts, as well as conventional notions of 'state' and 'non-state' actors[69].

Associated with the characteristics of *Web 2.0* and contemporary W3 trends, the effortless propagation, dissemination and redistribution of information via online communities is a prevailing modern trend[70]. Underground hacking communities encourage tool sharing, code

[60] Wong, (2008)
[61] Lambert, (2012:8)
[62] *ibid.*
[63] Elgin *et al.* (2012:1-6)
[64] Clarke, (2011)
[65] Rasheed, (2009:4)
[66] NCIX, (2011:1)
[67] NCIX, (2011:1-5)
[68] Rid cited in McGraw, (2012)
[69] Walton, (2008)
[70] Millard, (2012)

swapping, and the proliferation of malicious software, as well as facilitating *Dark Web* black-markets trading in zero-day vulnerabilities and stolen data[71]. These clandestine forums, what Villeneuve[72] describes as "malware ecosystems", consist of an array of programmers who understand network protocols, can write code, create viruses, malware, and rootkits, and who may even operate botnet infrastructures. There are also technicians who compile, package, and effectively utilise pre-built, open source, hacking tools, the so-called novice 'Script-kiddies', and surreptitious traders who actually buy and sell stolen data[73].

In line with the post-territorial, founding philosophy of the Internet[74], Sanderson describes how large-scale adoption of CMC has dissolved boundaries of physical locality and consequentially our understanding of 'community'[75]. Wellman and Gullia[76] suggest such virtual arenas "foster the formation of social networks and personal communities", but that such environments are distinctly insular and retreatist[77]. *Wiktorowicz* points to primary social contact occurring within small, introverted, clandestine dynamics, as cultivating high-risk behaviours[78]. Suler[79] highlights how the *dissociative anonymity* of W3 mitigates ones accountability whilst reducing inhibitions. Freed from societal checks and balances of normative behavioural conduct, Turkle[80] notes how such online communities allow users to put "fantasies-into-action"[81]. Such 'enabling environments' have successfully blurred lines between criminal exploitation and political espionage, making digital forensics and the ascription culpability an increasingly complex task[82].

Some states have proactively exploited this ambiguity to provide *plausible deniably* in committing hostile cyber acts. Utilising freelance, criminal, or independent 'patriotic' hackers to augment state operations seeking to spy upon or compromise foreign governments, military, industrial, and economic assets has muddied the water further[83]. Whilst the vast majority of purportedly state-sponsored cyber attacks have been for the purpose of

[71] Sageman *et al.*(2008:1347-1349)
[72] Villeneuve, (2010)
[73] Eli, (2010)
[74] Goldsmith & Wu, (2006:16-25)
[75] Sanderson & Fortin, (2001)
[76] *cited in* Steinkuehler, (2006:1)
[77] Jenny, (2008)
[78] *Wiktorowicz*, (2002); Millard, (2012)
[79] Suler, (2004)
[80] Turkle, (1995:226); Millard, (2012)
[81] Jones, (2006:104)
[82] Villeneuve, (2010); Richardson, (2006:21-36)
[83] Rid, (2012:20)

espionage, the very notions of 'state' and 'non-state' actors are not as patent as often assumed[84]. Henderson's research into the Red Hacker Alliance (RHA) is an interesting case in point[85]. Although RHA's assertion of being an independent union of hackers appears correct, the terminology and cultural disparity of the inquiry is fundamentally flawed, and concluding the Chinese state and RHA are disassociated is decidedly misleading. Walton[86] explains the difficulty arises by formulating distinctions based upon Western "liberal, democratic conception[s] of the nation-state". Cultural biases assume that elements of Chinese society acting 'autonomously' imply a disconnect from the state, and conversely, cyber-espionage entails the briefing, mobilisation, and supervision of the state.

The *People's Republic* of China consider the populace a fundamental facet of what it terms "comprehensive national power", featuring prominently within the Communist Party's rhetoric and strategic calculations[87]. The "masses" are viewed as both essential *to*, and responsible *for*, Chinese national security[88]. The mobilisation of civilians alongside the military is embodied in the Maoist concept of "the people's war", a philosophy retained in modern Chinese culture, with potential import to many ex-Soviet countries also[89]. Therefore, the 'non-state-status' of RHA may be theoretically true, but to say they are not advantageously concomitant, or that at the point of engagement and data extraction the two are even culturally and strategically separable, is mistaken. Although not one monolithic entity, this "non-traditional relationship" with the hacking fraternity is proactively sought as such groups can mount sophisticated operations against foreign targets[90]. Intelligent, skilled and patriotic, overheads are kept low and they are easily disowned if indentified. The information elicited may be extremely valuable and the damage caused substantial, it is clearly prudent to have such efforts focused overseas, rather than domestically.

Discovered in 2009, *Gh0stNet* provides a further example of state and non-state ambiguity[91]. The spying network infected high-value political and economic targets in 103 countries, infiltrating the networks of embassies, foreign ministries, NGOs, and government

[84] *ibid;* Edensor, (2001)
[85] Henderson, (2008)
[86] Walton, (2008)
[87] Henderson, (2008); Hutton, (2007)
[88] *ibid.*
[89] *ibid.*
[90] *ibid.*
[91] Glaister, (2009)

departments[92]. Spear-phishing emails targeted organisations with malicious attachments, which delivered the payload onto their system when opened. By leveraging *Web 2.0* and cloud based technologies as mechanisms of command-and-control, Gh0stNet was designed to maintain influence over compromised machines, even if the infrastructure was taken down[93]. The malware would connect to Google groups, Twitter accounts, or Blogspot threads, to obtain the instructive domain name – if this server was taken down, new IP addresses were reposted allowing the infiltration to continue[94]. The two-stage dropper would often instruct the installation of Gh0stRat, which allowed hackers to gain real-time control of computers, activating webcams and audio-recording to enable surveillance[95]. Gh0stNet's exposure revealed an infrastructure largely based in China with some interesting twists. One of the four control servers were located on Hainan Island, home to Lingshui Air Base signal-intelligence facility[96], two in and around Chengdu, a city dominated by the Triad mafia cartel[97], and the fourth was a government server[98].

Social Engineering and Non-technical Vectors

One of the most renowned cyber-espionage cases, the breach of global aerospace, defence, and advanced technology company Lockheed Martin, is also an excellent example of social engineering. Although breached in 2011, the preparation for the attack stretches back much further, encompassing the infiltration of two additional companies prior, originating with the successful hack of a relatively small and unprotected recruitment company called Beyond[99]. Impersonating the Beyond webmaster, spear-phishing techniques targeted their client; the network security company RSA who produce the *SecurID* authentication token used by Lockheed Martin. This is a complex mechanism of two-factor authentication, utilising a cryptography algorithm which generates a random code at fixed intervals, and is used by companies wishing to introduce a strong layer of security to their networks[100]. The vector of infection was an attached Microsoft Excel spreadsheet which stated: "I forward this file to you for review"[101]. Upon opening the attachment a Flash

[92] Markoff, (2009)
[93] Villeneuve, (2010); Nagaraja, & Anderson, (2009)
[94] IWM,.(2009)
[95] Markoff,.(2009)
[96] Harvey,.(2009); Hsiao;.(2010); GS,.(2011)
[97] Villeneuve, (2010); Nagaraja, & Anderson, (2009)
[98] Akkad, (2012)
[99] Schneier, (2011b)
[100] RSA, (2012)
[101] Clarke, (2011); Schneier, (2011a); Hodge & Sherr, (2011)

exploit embedded in the spreadsheet launched into RSA's network, utilising the *W32/Poison.Ivy* backdoor[102]. The payload gave a command-and-control server in Seoul, South Korea (119.70.119.30) remote access to the infected machines, enabling hackers to leapfrog into RSA's network and access the cherished algorithm which underpinned *SecurID*[103]. In 2011, Lockheed Martin announced that a cyber attack had successfully bypassed their security systems and managed to access "sensitive materials"[104]. Whilst the nature of information compromised was never extrapolated upon, the following month the U.S. Government redefined *casus belli* for an act of war to include cyber attacks[105].

The Lockheed Martin case was remarkable due to its complexity, strategic nature, and intelligent use of both human and cyber exploits, yet some are notable due to their simplicity and utility of non-technical infection vectors. The 2008 compromise of the Pentagon's top secret network occurred by *baiting* techniques of scattering infected USB thumb-drives in government carparks, then simply waiting for staff to pick one up, take it into work, and connect to a secure network[106]. Other traditional, 'non-cyber' means of obtaining intelligence to socially engineer convincing cyber-espionage attacks include; Freedom of Information requests, pitching marketing services, conferences, conventions, tradeshows, exploiting collaborative research ventures, and open sources.

Dubbed Operation Aurora, the 2010 exploitation of zero-day vulnerabilities in Microsoft's Internet Explorer, employed crucial social engineering elements, compromising numerous U.S. corporations including Google, Yahoo, Symantec, Northrop Grumman, and Morgan Stanley[107]. Staff were sent messages supposedly from known colleagues which included bogus weblinks. Once clicked, the malicious code launched, allowing hackers to piggyback from local machines into the entire network[108]. Whilst much of press coverage reported the infiltration of Chinese dissident gmail accounts, Dmitri Alperovitch of cyber investigation firm CrowdStrike, believes they accessed far more, claiming the Chinese are "hacking every company imaginable… stealing everything they need to capture business and market share". The breach is widely considered a "watershed moment", in so much as it

[102] Schneier, (2011b); Peter, (2011)
[103] Oquendo, (2011)
[104] Wolf, (2011); Lockheed Martin, (2011)
[105] Sanger & Bumiller, (2011)
[106] Mello, (2010)
[107] Paul, (2010); Naraine, (2010)
[108] Kurtz, (2010)

demonstrated that private industry and commerce had become as important, if not more so, than military or government targets in global cyber-espionage efforts[109]. Today, the assets most besieged include; information and communications technologies, marine systems**,** aerospace/aeronautics, military, dual-use and clean technologies, advanced materials and manufacturing techniques, pharmaceuticals, and agricultural technologies[110].

Conclusions and Recommendations

Technological developments and the increasing number of internet facing systems have seen the enthusiastic adoption of cyber means to illicitly obtain vast libraries of sensitive data. The expansion of online hacker communities, the emergence of W3 black-markets trading in espionage tools, technical instruction, and stolen data, as well as the utility of Web 2.0, have seen the blurring of criminal and political motivations. Historically and culturally grounded factors have distorted traditional Western notions of 'state' and 'non-state' actors, further confusing conceptions of what 'state sponsorship' entails. These dynamics, combined with the technically distributed, largely anonymous nature of attacks, have obscured attempts to precisely attribute responsibility for cyber-espionage offenses.

Rightly considered one of the most advanced persistent threats to information security today, costing billions annually in innovation, research, development, and lost revenue, this paper draws attention to some of the inconsistencies, inaccuracies and (in)competencies associated with documenting and measuring the cost of cyber-espionage. However, whilst cost estimations may vary so wildly as to render them an almost redundant exercise, undeniably it will always be faster and cheaper to steal intellectual property, trade secrets, or acquisition information than to fund it directly. In line with the dialects of globalisation, late-modernity, and transnational capitalism, economic competiveness and national advantage have seamlessly merged. Therefore, not only are the motivations patent, the perpetrators determined, and the data losses gigantic, but the economic, social, and political ramifications are enormous also.

In our current climate of austerity measures, efficacy drives, and stagnant growth — alongside the emergence of new global powers and the scramble for finite world resources — a nation's research, innovation, and economic competitiveness is as critical to

[109] Faber, (2012)
[110] NCIX, (2011:1)

guaranteeing the future security and prosperity of the country, more so even, than military strength alone. Indeed, the anonymous and often surreptitious nature of cyberspace has lent itself to espionage in ways perhaps not immediately applicable to warfare, where political oratory, drum beating, and flag flying are inherently part and parcel.

This analysis underscores that cyber-espionage is not merely a matter of hugely complicated code silently pilfering data in the background of networks. Non-technical methods, social engineering techniques, and the efficacy of human exploits, are still tremendously important and must not be overlooked as the cyber-security hysteria grips academics, practitioners and policymakers on either side of the Atlantic. Espionage is nothing new, but the capability, persistence, and magnitude of the threat has changed significantly, our responses must be commensurate but composed, effective not foolish. It is the nexus and interplay between the technological, economic, cultural, and geopolitical shifts which provide a more nuanced understanding of espionage.

Given its restrictive parameters, this paper should by no means be viewed as a exhaustive account detailing every facet of cyber-espionage, but rather a cursory analysis of this novel yet ubiquitous threat. Analytical perspectives from political and social sciences have significant import to cyber-security and can afford us some pertinent insights. Combining these with comprehensive technical analysis from computer science, assessing core vulnerabilities, best-practise solutions, and rethinking architectural and software design is essential. This paper seeks to promote multidisciplinary research within this rapidly developing field, bridging the knowledge-gap between technologists, academics, policy makers, lawyers, and industry. Encouraging research driven, empirically informed, and theoretically conversant countermeasures, seeking to reduce cyber-espionage and, ultimately, bolster our information security.

Bibliography

Ahlgren, B (2005) 'Trends in the evolution of the Internet Architecture', Swedish Institute of Computer Science, {Online resource} Available at: http://winternet.sics.se/workshops/grandfinale/Ahlgren.pdf [Accessed 03/11/2012]

Albanesius, C. (2012) 'Massive Flame: Malware Stealing Data Across Middle East', PC Magazine, 28th May {Online resource} Available at: http://www.pcmag.com/article2/0,2817,2404951,00.asp, [Accessed 20/11/12]

Alexander, K. (2012) 'Cybersecurity: Threats to the US', American Enterprise Institute, C-Span, {Online Resource} Available at:http://www.c-spanvideo.org/program/306956-1 [Accessed 06/11/12]

American Enterprise Institute (2012) 'Cybersecurity Threat to The US', American Enterprise Institute, C-Span Video Library, {Online Resource} Available at: http://www.c-spanvideo.org/program/306956-1 [Accessed 27/10/12]

Anuradha, S (2011) 'Huawei maintained steady growth in 2010', Computerworld, 18th April, {Online Resource} Available at: http://news.idg.no/cw/art.cfm?id=2A72801F-1A64-67EA-E484130BD34FD158 [Accessed 20/11/12]

Appadurai, A. (1990) 'Disjuncture and difference in the global culture economy', Theory, Culture, and Society, (7):295-310

Bauman, Z. (2000) 'Liquid Modernity', Cambridge: Polity

Berners-Lee, T (1990) 'Bio', World Wide Web Consortium, {Online resource} Available at: http://www.w3.org/People/Berners-Lee/ [Accessed 02/03/2012]

Boomberg (2011) 'Huawei 2010 Profit Gains 30% on Higher International Sales', Bloomberg, 17th April, {Online Resource} Available at: http://www.bloomberg.com/news/2011-04-17/huawei-technologies-profit-rises-30-led-by-higher-international-sales.html [Accessed 17/11/12]

Brachman, J. (2008) Global Jihadism: Theory and Practice, Taylor & francis

Clarke, R (2011) 'Cyber Warfare', Honors Colloquium, University of Rhode Island, {Online Resource} Available at: http://www.youtube.com/watch?v=wRttZgeTrZQ&list=PLJE-LFTjhw0IYAAxkHdaVfFL_tr73CN4g&index=1&feature=plpp_video[Accessed 12/11/12]

Clarke, R. (2010) 'Cyber War', New York: Harper Collins

Clausewitz, Von C. (1832) 'On War', English translation by Howard, M. & Paret, P. (1976/84), Princeton: University Press

Cohen, S. (1972) 'Folk Devils and Moral Panics', London: MacGibbon & Kee

CrySyS Lab (2012) 'sKyWIper: A Complex Malware for Targeted Attacks', Budapest University of Technology and Economics, Laboratory of Cryptography and System Security, 28th May, {Online resource} Available at: http://www.crysys.hu/skywiper/skywiper.pdf, [Accessed 20/11/12]

Dalgaard-Nielsen, A. (2010) 'Violent Radicalization in Europe: What We Know and What We Do Not Know', Studies in Conflict and Terrorism, 33(9):797-814.

Detica (2012) 'The Cost of Cyber Crime: a Detica report in partnership with the Office of Syber Security and Information Assurance in the Cabinet Office, {Online Resource} Available at: http://www.baesystemsdetica.com/uploads/press_releases/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf [Accessed 27/11]

Edensor, T. (2001) 'National Identities and Popular Culture', Oxford: Berg

Elgin, B., Lawrence, D. & Riley, M. (2012) 'Coke Gets Hacked And Doesn't Tell Anyone', Bloomberg News, 4th Nov, {Online Resouce} Available at: http://www.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html [Accessed 06/11/12]

Eli The Computer Guy (2010) *'Hacking for Beginners'*, {Online resource} Available at: http://www.youtube.com/watch?v=yGIHjTmTFfA [Accessed 10/11/2012]

Erdbrink, T. (2012) 'Iran Confirms Attack by Virus That Collects Information', The New York Times, 29th May, {Online resource} Available at: http://www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html?_r=1&hp, [Accessed 20/11/12]

Evans, J (2012) 'The Olympics and Beyond', {Online Resource} Avilable at: https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/director-general/speeches-by-the-director-general/the-olympics-and-beyond.html [Accessed 12/11/12]

Faber, D.(2012) 'Cyber Espionage: The Chinese Threat', CNBC Investigates, 9th July, {Online Resource} Available at: http://www.youtube.com/watch?v=iqz1QgraG_o, [Accessed 07/11/12]

Foryst, C. (2010) 'Rethinking National Security Strategy Priorities', International Journal of Intelligence and Counter-Intelligence, 23(3): 399-425

Giddens, A. (1991) 'Modernity and Self-identity: Self and Society in the Late Modern Age', Cambridge: Polity

Glaister, D. (2009) 'China accused over global computer spy ring', 30th March, The Guardian, {Online Resouce} Available at: http://www.guardian.co.uk/world/2009/mar/30/china-dalai-lama-spying-computers [Accessed 24/11/12]

Goldsmith, J. & Wu, Tm (2006) 'Who controls the internet? : Illusions of a borderless world', London: Oxford University Press

Gorman, S. (2012) 'Chinese Hackers Suspected In Long-Term Nortel Breach', Wall Street Journal, 14th February, {Online Resource} Availble at: http://online.wsj.com/article/SB10001424052970203363504577187502201577054.html, [Accessed 26/11/12]

Gostev, A (2012) 'The Flame: Questions and Answers', Securelist, {Online resource} Available at: https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers, [Accessed 20/11/12]

Gralla, P. (2007) 'How the Internet Works', 8th Ed, 2011, Indiana: Que Publishing

Gross, M. (2011) 'A Declaration of Cyber-War', Vantiy Fair, April, {Online Resource} Available at: http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104 [Accessed 14/11/12]=

GS,.(2011) 'Lingshui Air Base', Global Security, 7th Nov, {Online Resource} Available at: http://www.globalsecurity.org/military/world/china/lingshui.htm [Accessed 01/12/12]

Harvey, M. (2009) 'Chinese hackers using ghost network to control embassy computers'. The Times (London), 29th March, {Online Resource} Available at: http://www.timesonline.co.uk/tol/news/uk/crime/article5996253.ece [Accessed 01/12/12]

Henderson, S (2008) *'Beijing's Rising Hacker Stars: How Does Mother China React?'*, IO Sphere, Fall Ed., Foreign Military Studies Office/Joint Regional Intelligence Center, {Online resource} Available at: http://fmso.leavenworth.army.mil/documents/Beijings-rising-hackers.pdf [Accessed 10/11/2012]

Hodge, N & Sherr, I.(2011) 'Lockheed Martin Hit By Security Breach', Wall Street Journal, 27th May, {Online Resource} Available at: http://online.wsj.com/article/SB10001424052702303654804576350083016866022.html?mod=WSJ_hp_LEFTWhatsNewsCollection [Accessed 04/04/12]

Hsiao, R. (2010) 'China's Cyber Command?', The Jamestown Foundation, China Brief, 22nd July, 10(15): {Online Resource} Available at: http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=36658&tx_ttnews%5BbackPid%5D=414&no_cache=1 [Accessed 01/12/12]

Hutton, W. (2007) The Writing on the Wall: China and the West in the 21st Century, Little Brown:London

Internet World Statistics (2012) 'The Internet Big Picture: World -Internet Users and Population Stats', Minwatts Marketing Group, {Online Resource} Available at: http://www.internetworldstats.com/stats.htm [Accessed 25/10/12]

IWM,.(2009) Tracking GhostNet: Investigating a Cyber Espionage Network', Information Warfare Monitor, 29th March, {Online Resource} Available at:http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network [Accessed 28/11/12]

Janis, I. (1972) 'Victims of groupthink', Boston: Houghton Mifflin

Jenny, R. (2008) 'The Virtual Campfire: An Ethnography of Online Social Networking'. {Online resource} Available at: http://www.thevirtualcampfire.org/ [Accessed 21/12/2011]

Jones, S, (1995) 'Understanding Community in the Information Age' in Jones, S. (Ed.) Cyber Society: Computer Mediated Communication and Community, Thousand Oaks: Sage

Jones, S. (2006) 'Criminology', 3rd Ed, Oxford: Oxford University Press

Kindlund, D. (2012) 'Flamer/sKyWIper Malware: Analysis', FireEye, 30th May {Online resource} Available at: http://blog.fireeye.com/research/2012/05/flamerskywiper-analysis.html, [Accessed 20/11/12]

Knight, G. (2003:15) 'Internet Architecture', University College London: University Press, {Online resource} Available at: http://www.cs.ucl.ac.uk/staff/g.knight/LectureNotes/InternetArchitecture.pdf [Accessed 04/03/2012]

Kurtz, G. (2010) 'Operation "Aurora" Hit Google, Others', 14th Jan, McAfee, {Online Resource} Available at: http://blogs.mcafee.com/archive/operation-aurora-hit-google-others [Accessed 22/11/12]

Lambert, P. (2012) 'Analysis of a targeted cyber attack', Tech Republic, 8th Nov, {Online Resource} Available at: http://www.techrepublic.com/blog/security/analysis-of-a-targeted-cyber-attack/8633 [Accessed 24/11/12]

Lee, D. (2012) 'Flame: Massive Cyber-Attack Discovered, Researchers Say', BBC News, 28th May. {Online resource} Available at: http://www.bbc.co.uk/news/technology-18238326, [Accessed 20/11/12]

Lockheed Martin (2011)'Lockheed Martin Customer, Program And Employee Data Secure', Press Release, 29th May, {Online Resource} Available at: http://www.lockheedmartin.com/news/press_releases/2011/0528hq-secuirty.html, [Accessed 04/12/12]

Maass, P. & Rajagopalan, M. (2012) 'Does Cyber Crime Really Cost $1 Trillion?', Pro Publica, 1st August, {Online Resource} Available at: http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion [Accessed 26/11/12]

Markoff, J. (2009) 'Vast Spy System Loots Computers in 103 Countries', The New York Times, 28th March, {Online Resource} Avilable at: http://www.nytimes.com/2009/03/29/technology/29spy.html [Accessed 20/11/12]

McAfee Labs (2011) ' Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency', {Online Resource} Available at: http://www.mcafee.com/us/resources/reports/rp-underground-economies.pdf [Accessed 20/11/12]

McAfee Labs (2012) 'McAfee Threats Report: Second Quarter 2012', {Online Resource} Available at: http://www.mcafee.com/uk/resources/reports/rp-quarterly-threat-q2-2012.pdf [Accessed 20/11/12]

McGraw,G.(2012) 'Show 080 - An Interview with Thomas Rid', Cigital, Silver Bullet podcast series, 30th Nov, {Online Resource} Available at: http://www.cigital.com/silver-bullet/show-080/ [Accessed 02/12/12]

Mello, JP (2010) 'Pentagon: Yep, We Got Hacked', TechNewsWorld, 26th August, {Online Resource} Available at: http://www.technewsworld.com/story/70699.html [Accessed 04/12/12]

Nagaraja, S. & Anderson, R. (2009) 'The snooping dragon: social-malware surveillance of the Tibetan movement', Technical Report 746, Cambridge University Computer Laboratory, {Online Resource} Available at: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf [Accessed 28/10/12]

Naraine, R. (2010) 'Microsoft knew of IE zero-day flaw since last September', Zero Day, 21st Jan, {Online Resource} Available at: http://www.zdnet.com/blog/security/microsoft-knew-of-ie-zero-day-flaw-since-last-september/5324 [Accessed 27/11/12]

NCIX (2011) 'Foreign Spies Stealing US Economic Secrets in Cyberspace', Report to Congress on Foreign Economic Collection of Industrial Espionage 2009-2011, Oct 2011, Office of the National Counterintelligence Executive, {Online Resource} Available at: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf [Accessed 21/11/12]

Neumann, P. & Rogers, B. (2007) 'Recruitment and mobilisation for the Islamist militant movement in Europe', ICSR, Kings College: University of London Press, {Online resource} Available at: http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/ec_radicalisation_study_on_mobilisation_tactics_en.pdf, [Accessed 01/12/2011]

ODO (2012) 'Oxford Online Dictionary', {Online Resource} Available at: http://oxforddictionaries.com/definition/english/Internet [Accessed 25/10/12]

Oquendo, J.(2011) 'Shady Rats and Poison Ivy', inf!ltrated.net, {Online Resource} Available at: http://infiltrated.net/index.php?option=com_content&view=article&id=42&Itemid=48 [Accessed 04/12/12]

Panetta, L. (2012) 'Defending the Nation from Cyber Attack', Business Executives for National Security, NYC USS Intrepid, Global News {Online Resource} Available at: http://www.youtube.com/watch?v=ttZLBufYbu0 [Accessed 07/11/12]

Paul, R.(2010) 'Researchers identify command servers behind Google attack', ARStechnica, 14th Jan, {Online Resource} Available at: http://arstechnica.com/security/2010/01/researchers-identify-command-servers-behind-google-attack/ [Accessed 25/11/12]

Peter, TA. (2011) 'How bad was the cyber attack on Lockheed Martin?' The Christian Science Monitor, Terrorism & Society, 29th May, {Online Resource} Available at:http://www.csmonitor.com/World/terrorism-security/2011/0529/How-bad-was-the-cyber-attack-on-Lockheed-Martin, [Accessed 04/12/12]

Rasheed, A. (2009) 'Iraq signs deal with BP, CNPC for Rumaila field', Reuters, 8th Oct, {online resouce} Available at: http://www.reuters.com/article/2009/10/08/iraq-oil-idUSL820863520091008 [Accessed 24/11/12]

Rawnsley, G. (2011) 'MI5 alert on China's cyberspace spy threat', {Online Resource} Avilable at: http://ics-www.leeds.ac.uk/papers/vp01.cfm?outfit=gdr&folder=32&paper=106 [Accessed 26/11/12]

Rid, T. (2012) 'Cyber War Will Not Take Place', Journal of Strategic Studies 35(1): 5-32

Rogers, M. et al. (2012) 'Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE', House Permanent Select Committee on Intelligence, 8th October, U.S. House of Representatives 112th Congress, {Online Resource} Available at: http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf [Accessed 20/11/12]

Roudometof, V (2005) 'Translationalism, Cosmopolitanism, and Glocalization', Current Sociology 53 (1): 113–135.

RSA,.(2012) 'Hardware Authenticators', EMC Corporation, {Online Resource} Available at: http://www.emc.com/security/rsa-securid/rsa-securid-hardware-authenticators.htm#!offerings [Accessed 02/12/12]

Sageman, M., Chen, H., Chung, W., Qin, J., Reid, E., & Weimann, G. (2008) Uncovering the DarkWeb: A Case Study of Jihad on the Web, Journal of the American Society for Information Science & Technology, 59(8):1347–1359

Sanderson, D. & Fortin, A. (2001) 'The Projection of Geographical Communities into Cyberspace' in Munt, SR. (2001) 'Technospaces: Inside the New Media', London: Continuum

Sanger, DE. & Bumiller, E. (2011) 'Pentagon to Consider Cyberattacks Acts of War', The New York Times, 31st May, {Online Resource} Available at: http://www.nytimes.com/2011/06/01/us/politics/01cyber.html [Accessed 04/12/12

Schneier, B.(2011a) 'Lockheed Martin Hack Linked to RSA's SecurID Breach', Schneier on Security, 30th May, {Online Resource} Available at:http://www.schneier.com/blog/archives/2011/05/lockheed_martin.html [Accessed 04/12/12]

Schneier, B.(2011b) 'Details of the RSA Hack', Schneier on Security, 30th Aug, {Online Resource} Available at:http://www.schneier.com/blog/archives/2011/08/details_of_the.html [Accessed 04/12/12]

Shipman, M. (1997) 'The Limitations of Social Research', 4th Ed, London: Longman

Steinkuehler, C. & Williams, D (2006) 'Where everybody knows your (screen) name: Online games as third places', Journal of Computer-Mediated Communication, 11(4): 1 , {Online resource} Available at: http://jcmc.indiana.edu/vol11/issue4/steinkuehler.html [Accessed 21/12/2009]

Stevens, T. & Neumann, P. (2009) 'Countering Online Radicalisation: A Strategy for Action', ICSR, Kings College: University of London Press

Suler, J. (2004) 'The Online Disinhibition Effect', Cyber-Psychology & Behavior, 7 (3):321–326

Sutherland, E. (1947) 'Principles of Criminology', 4th Ed, Philadelphia: Lippincott

Symantec (2012) 'State of Information: Global Results' {Online Resouce} Avilable at: http://www.symantec.com/content/en/us/about/media/pdfs/2012-state-of-information-global.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Jun_worldwide_StateofInformation, [Accessed 20/11/12]

Thomas, T. (2005) 'Cyber Silhouettes: Shadows over Information Operations', Foreign Military Studies Office (FMSO), Kansas: Fort Leavenworth Press

Thornburgh, N. (2005) 'The invasion of the Chinese cyberspies', Time Magazine, 29th Aug, {Online Resource} Available at: http://www.time.com/time/magazine/article/0,9171,1098961,00.html

Turkle, S. (1995) 'Life on the Screen: identity in the age of the internet', London: Phoenix.

Vance, A. & Einhorn, B. (2011) 'At Huawei, Matt Bross Tries to Ease US Security Fears', Bloomberg Businesweek, {Online Resouce} Avialble at: http://www.businessweek.com/magazine/at-huawei-matt-bross-tries-to-ease-us-security-fears-09152011.html [Accessed 27/11/12]

Verizon, (2012) '2012 Data Breach Investigations Report', Verizon RISK Team, {Online Resource} Availabl at: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf [Accessed 22/11/12]

Villeneuve, N. (2010) 'Shadows in the Cloud - Investigating Cyber Espionage 2.0', Palantir Government Conference, GovCon5, Tyson Corner VA {Online Resource} Available at: http://www.youtube.com/watch?v=o3HQ29AUo6Q&playnext=1&list=PL6JOrUIbT84jzkIn7WWuOupnTT4Gq9Kag&feature=results_video [Accessed 12/11/2012]

Walton, G (2008) 'Year of the Gh0st RAT: Trading with China, what risks, responsibilities, opportunities?', Openflows Panel Discussion 4, Beijing Olympic 2008: Winning Press Freedom Paris Conference, {Online resource} Available at: http://www.w3.org/People/Berners-Lee/ [Accessed 10/11/2012]

Wessels, B (2009) 'Understanding the internet: a socio-cultural perspective, Basingstoke

Wiktorowicz, Q. (2002) 'Social Movement Theory and the Study of Islamism: A New Direction for Research' Mediterranean Politics, 7(3): 187-211.

Wolf, J.(2011) 'Lockheed says frequent cyber target from around the world', Reuters, 29th May, {Online Resource} Available at: http://www.reuters.com/article/2011/05/29/us-usa-defense-hackers-idUSTRE74Q6VY20110529 [Accessed 04/12/12]

Wong, S. (2008) 'Coca-Cola to Buy China's Huiyuan for $2.3 Billion (Update4)', Bloomberg News, 3rd Sept, {Online Resource} Available: http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aI9_PX_Btrqs&refer=home [Accessed 23/11/12]

Zetter, K. (2012) 'Meet Flame - The Massive Spy Malware Infiltrating Iranian Computers', Wired, 28th May, {Online resource} Available at: https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers, [Accessed 20/11/12]