The Cyber-Industrial-Complex

What does the militarisation of the 'fifth domain' entail and what are the consequences?

http://www.henrysevers.com

The Cyber-Industrial-Complex: What does the militarisation of the 'fifth domain' entail and what are the consequences?

Henry Severs

Focus and Limitations

This paper examines the consequences of a growing pressure and increased enthusiasm for governments, armed services, and commercial actors to develop and operationalise military capabilities in cyberspace.

Analysis is approached through five convergent lines of enquiry. To provide context, the development of the internet from a 'tool' to a 'territory' shall be discussed, exploring the various technological, demographic, and social shifts brought about by this evolution. Next, the geostrategic influence of cyber threats shall be touched upon, describing the economic, legal, and strategic affects profoundly influencing perceptions of cyberspace. This will be followed by the ways in which governments have sought to securitise cyberspace, highlighting the various budgetary and operational considerations driving the militarisation of the 'fifth domain'. A discussion of 'cyber-doom' narratives and threat inflation regarding cyber attacks shall then be presented, critiquing discourses and drawing parallels with Weapons of Mass Destruction (WMDs). Finally the amalgamation of political, military, and commercial interests within the emergent 'cyber-industrial-complex' shall be examined. In concluding, many of the consequences and implications facing policymakers shall be considered, and the call for further research-driven, sober policymaking such be made.

Throughout, reference shall be made to relevant case studies, and conceptual frameworks from the social sciences. The argument shall be made that not only is the cyber-industrial-complex increasing in reach and intensity, but faith that the militarisation of the fifth domain will achieve effectual cyber security is misplaced. Ultimately the top-down control of cyberspace, at odds with prevailing internet trends, is argued to be an expensive means to achieve ineffectual results.

Inherent limitations when exploring a relatively young, multi*disciplinary* field, examining a rapidly evolving topic, must be acknowledged at this preliminary stage[1]. Themes discussed are not presented as static social truths, but more akin to Weberian 'ideal typical' discourses[2]. Despite this papers validity and application, it is a cursory examination of the cyber-industrial-complex intended to stimulate debate, and caution should be exercised in making wider generalisations[3]. In order to effectively address the question and avoid tangential theoretical debates, the utility of explicitly expressed working definitions is critical – appreciating more suitable vernacular may develop[4]. Throughout, *'the internet'* is taken as the "global computer network, providing a variety of information and communication facilities, consisting of interconnected [network of] networks using standardised communication protocols"[5]. Here, Stevens'[6] definition of *'cyberspace'* as the "total landscape of technology mediated communication" is utilised. It takes Cramer and Thrall's depiction of 'threat inflation' as the creation of "concern for a threat that goes beyond the scope and urgency [a]… disinterested analysis would justify"[7].

From Tool to Territory

To contextualise changing attitudes and perceptions towards cyberspace, it is important historically ground this evolution. In 1937, futurist H.G. Wells hypothesised the future development of an international encyclopaedia, or *World Brain*, encompassing the sum of human knowledge. In the 1960s Joseph Licklider, first head of Defense Advanced Research Projects Agency Network (DARPA), envisioned a 'Galactic Network' of globally connected computers, through which anyone could access information. Advancements in packet switching, standardisation of Internet protocol, and the expanded connection of ARPANET to include research and education institutions in the 1970/80s, saw the Wells' vision being plausibly discussed for the first time. The commercialisation of the internet occurred in the 1990s, as final traffic restrictions were lifted[8].

[1] Shipman, (1997)
[2] Poggi, (2006)
[3] NCIX, (2011:i-iii)
[4] Shipman, (1997:16)
[5] ODO, (2012); Gralla, (2007:7)
[6] Stevens & Neumann, (2009:10)
[7] Crammer & Thrall, (2009)
[8] Greene *et al.*(2003)

Today cyberspace is almost unrecognisable from earlier manifestations, now fully entrenched in all facets of modern life, culture, and commerce. The astonishingly rapid growth of cyberspace, from a research tool used by a few, to the ubiquitous framework sustaining global societies is unparalleled[9]. Widely considered a catalyst for globalisation, the rise of the internet concomitant to the ascension of the information based economy, will doubtless come to epitomise this era of history as the enlightenment and industrial revolution has preceding centuries[10]. The internet has transformed and revolutionised: employment, trade, culture, innovation, politics, research, education, development, sociality, information access, and, most notably, the communications landscape. In 1993 1% of the world communicated through two-way telecommunications, by 2000 this had risen to 51%, in 2007 it was 97%[11]. Internet penetration exploded from 360 million in 2000, to 2.4 billion in 2012 – an extraordinary 556% rise[12]. The world population is on course to reach 7.3 billion by 2016, with mobile internet devices exceeding 10 billion[13]. The volume of SMS messages tripled between 2007 and 2010, topping 6.1 trillion, averaging 200,000 messages per second[14].

Beyond enormous technical enhancements[15], cyberspace is experiencing a demographical shift, as the pendulum of internet concentration swings from the global North to the South, challenging traditional Western hegemony[16]. While cyberspace may be indigenously American, countries such as China, India, and Brazil will come to outnumber the early 'digital natives' within our lifetime[17]. Asia constitutes 42% of the planet's internet population (#1), but enjoys only 21.4% penetration (#6), illustrating the enormous potential for connectivity[18]. Of 5.3 billion mobile subscriptions in 2010, 3.8 billion were from the developing world, and 18/55 highest internet penetrating countries are the “poorest and weakest of the international community”[19].

Inevitably new demographics bring fresh cultural, social, political, and strategic priorities. Cyberspace is now widely acknowledged as a “commons” where people socialise, engage,

[9] Deibert & Crete-Nishihata, (2012)
[10] Bauman, (2000); Severs-Millard, (2012ac)
[11] Hilbert & López, (2011)
[12] IWS, (2012)
[13] Alexander, (2012)
[14] Deibert & Rohozinski, (2011:23)
[15] IWS, (2012); Knight, (2003:15); Ahlgren, (2005); Edensor, (2001)
[16] Deibert, (2011); Deibert & Rohozinski, (2011:23); Deibert & Crete-Nishihata, (2012)
[17] Brito & Watkins, (2011); Lawson, (2011); Deibert & Rohozinski, (2011:26)
[18] IWS, (2010a); IWS, (2012)
[19] ITU (2010); IWS, (2010b); UN OHRLLS, (2011)

and organise, but also an environment in its own right[20]. In keeping with the pioneering, post-territorial aspirations of the internet[21], Sanderson and Fortin[22] observe large-scale adoption of cyberspace as dissolving physical confines and redefining core societal precepts. Renninger and Shumar[23] view the internet as a tool *and* a territory, facilitating users to assemble in a virtual arena, who otherwise are unable. Amit[24] describes shifting anthropological appreciations of the social environment, from tangible social forms, to emphasising the virtual. Cyberspace can no longer simply be viewed as a medium, or a medley of mediums, but as a "continent, rich in resources", possibilities, and challenges[25].

Geostrategic Influence

This shift towards perceiving cyberspace as a new environment transcending society, economics, and geopolitics, has resulted in nefarious actors seeking to exploit vulnerabilities to reap enormous personal and collective rewards[26]. Inevitably, this has drawn the attention of nation states, seeking to protect interests, whilst staking claim, and establishing control over this emergent terrain[27]. Governments have sought to delineate boundaries, through a myriad of legislation, whilst military and intelligence entities have scrambled to assert their own influence over this sphere[28]. Minimal barriers and relative anonymity of malicious actors, combined with the emergence of *Web 2.0* "malware ecosystems" propagating hacking tool-kits and botnets, have allowed determined groups – whether criminals, freelancers, or intelligence agencies – to make substantial gains beyond real world means[29].

Once the sole concern of an inner circle of technologists, internet control and security has become the preoccupation of nation states. The three primary cyber-threats concerning governments are: 1. Theft, corruption, manipulation or exploitation of information; 2. Disruption of accessibility to networks, data, or resources; 3. Destruction or degrading of

[20] Deibert & Rohozinski, (2011:24)
[21] Goldsmith & Wu, (2006:16-25)
[22] Sanderson & Fortin, (2001)
[23] Renninger & Shumar, (2002)
[24] Amit, (2002:3)
[25] Glenny, (2010)
[26] Hilbert, & López, (2011); Deibert & Rohozinski, (2011)
[27] *ibid.*
[28] Glenny,.(2010); Deibert, (2012); Deibert & Crete-Nishihata, (2012); Lynn, (2011)
[29] Villeneuve, (2010); Henderson, (2008); Andres, (2013); Alexander, (2011)

networks, infrastructure, and communications[30]. Within a geostrategic paradigm, such threats have profoundly influenced the militarisation of cyberspace[31]:

Firstly, the *economic burden*. The UK government placed the 2012 national cost of cybercrime at £27 billion, £16.8 billion being industrial espionage[32]. US intellectual property theft purportedly amounts to $250 billion per annum[33], cybercrime a further $114 billion, or $388 billion factoring in downtime[34]. McAfee[35] estimates global annual remediation costs to be an incredible $1 trillion, a statistic often cited despite being disputed by the very researchers ostensibly quoted[36]. The pilfering of sensitive information cost Coca-Cola their attempted takeover of Huiyuan Juice Group in 2009, producing losses in the region of $2.4 billion[37]. Nortel, once the world leading telecommunications supplier valued at $250 billion, declared bankruptcy in 2009 following a nine year data exfiltration[38]. The "astonishing" number of "industrial scale"[39] cyber-attacks targeting UK companies, prompted MI5 Director General, Jonathan Evans, to issue letters to the top 300 businesses stressing the threat of "electronic espionage"[40]. Although ascribing the true cost of cyber-attacks is extremely difficult, it is clear the costs are high, rising, and potentially may even influence the global balance of power[41].

Secondly, *obscuring political liability* by employing proxy servers, 'cyber militias', or freelance hackers[42]. Potentially creating a smokescreen for implanting 'logic bombs' into critical infrastructure, but primarily affording plausible deniability for acts at odds with the official political stance[43]. An interesting case is the oft-cited 2007 Estonian incident, where Russian 'patriotic' hackers launched a DDoS attack on banking and civil service systems. Russia inevitability denied responsibility, and attribution proved unsuccessful[44]. Nevertheless, Moscow achieved the same coercive ends, without serious diplomatic repercussions, essentially punishing Estonia whilst circumventing accountability[45]. In more

[30] Lord & Sharp *et al*.(2011:25-40;165-182)
[31] Andres, (2013)
[32] Detica, (2012)
[33] Symantec-Corp., (2012)
[34] Alexander, (2012)
[35] McAffe Inc., (2012)
[36] Maass & Rajagopalan,.(2011)
[37] Wong, (2008); Lambert, (2012:8); Severs-Millard, (2012c)
[38] *ibid.*
[39] Evans, (2012)
[40] Rawnsley, (2011)
[41] Severs-Millard, (2012); Clarke, (2010); Ottis, (2010)
[42] Andres, (2013); Henderson, (2008)
[43] NCIX, (2011:1)
[44] Czosseck, (2011)
[45] Andres, (2013)

pugnacious uses of cyber-militia by Russia during her conflict with Georgia, the sabotage of key Georgian communication systems, synchronised with kinetic military operations, further demonstrated the efficacy of deniability[46]. Had the military been directly implicated, Russia would have violated legal armed conflict doctrines, as cyber attacks on third-party states were necessary to disrupt Georgian systems[47]. Again, Moscow successfully sabotaged Georgia's communications whilst evading liability.

Thirdly, the rapidly transforming cyber-threat landscape, has *redefined the strategic perspective* of many governments. States now view cyberspace as a means to either augment or substitute their kinetic warfare capabilities. The 2007 Israeli bombing of the Syrian nuclear facility at Dayr az-Zawr provides an interesting case in point. By using UAVs similar to the ancillary US programme *Senior Suter*[48], Israel was able to hack air-defence systems and manipulate their radar to show a clear sky, allowing F15 fighter jets to carpet bomb the site and leave Syrian airspace without any resistance or retaliation[49]. Many governments are proactively seeking to develop their cyber-arsenals, creating numerous dedicated institutions to this end.

Militarising the Fifth Domain

The four-year, £650m, British *Cyber Security Strategy* emphasises protective, defensive, and 'pre-emptive' action: tackling cyber crime to ensure a secure business environment; improving system and software resilience; encouraging stable social arenas; and improving knowledge and skill-sets necessary to achieve these goals[50]. Provisions seek to raise public and commercial awareness, bolster law enforcement and cross-border collaboration, improve industry standards, and develop MoD and GCHQ capabilities[51]. Although emphasising target hardening and resilience, the offensive stance is evident.

> *"Defence Cyber Operation Group [is] to bring together cyber capabilities from across defence. The group will include a Joint Cyber Unit hosted by GCHQ… [to] develop new tactics, techniques, and plans to deliver military effects"*[52]

[46] *ibid.*
[47] Czosseck, (2011)
[48] Gasparre, (2008ab)
[49] Severs-Millard, (2012)
[50] Cabinet Office, (2011)
[51] Cabinet Office, (2012)
[52] Cabinet Office, (2012: 26[4.9])

Notions of 'pre-emptive defence' are echoed in the *NATO Strategic Concept*, where the language of prevention, detection, and defence blends with notions of military capability, operational reach, and strategic dominance[53]. This doctrine is most explicit in the US, where the *Strategy for Operating in Cyberspace: Priorities for 21st Century Defense* are candid about intentions to boost military capabilities and operational effectiveness in all realms – land, air, maritime, space, and the 'fifth domain', cyberspace[54]. This mission has fallen to *US Strategic Command* (USSTRATCOM), who established *US Cyber Command* (USCYBERCOM) to synchronise operations across the military sphere, including *Army Cyber Command*, *10th Fleet Cyber Command*, *24th Air Force*, and *Marine Corps Forces Cyber Command*. An interesting directorial feature is USCYBERCOM's dual locality within the NSA, and Gen. Keith Alexander being tri-hatted as *Director of NSA*, *Chief of the Central Security Service*, and *Commander of USCYBERCOM*.

In the 2013 US fiscal budget cyber capabilities take precedence; designating $3.4 billion for USCYBERCOM, with a total allocation of £18 billion through to 2017[55]. The Department for Homeland Security will spend: $345 million on the *National Cybersecurity Protection System* and EINSTEIN.3 – the intrusion detection and analytics system; $236 million on the *Federal Network Security Branch* to secure agency systems; $93 million on *U.S. Computer Emergency Readiness Team,* the operational wing of the *National Cyber Security Division*; $64.5 million on cyber investigations and computer forensics conducted by the *Secret Service*; and $12.9 million on virtual training and cyber-war games[56].

Although the tendency for governments to view the cyber-domain through a military lens may be more acute than ever, it is certainly not a recent theme[57]. The history of militarising cyberspace has been a gradual process concomitant to the technological, demographic, and social shifts previously discussed. ARPANET was originally funded by the US Department of Defense (DoD), the term "cyber-deterrence" was coined in 1994, and *'Eligible Receiver',* the first NSA cyber-war games were held in 1997[58]. The first public reference to "cyber-attack" and "information security risks" were made by former CIA

[53] NATO, (2010)
[54] Department of Defense, (2012a)
[55] Rosenberg, (2012); DoD, (2012b); DoD, (2012c)
[56] Roberts, (2012)
[57] Rid, (2012b:5-6)
[58] Clayton, (2011)

Director George Tenet in 1998, the same year cyber operations were consolidated under the *Computer Network Defense Joint Task Force*[59]. In 2003, the *National Cyber Security Division* was established, tasked with protecting government systems, and in 2006 plans for USCYBERCOM were announced. Perhaps then, using tactical or warfare rhetoric to describe objectives in cyberspace is somewhat inevitable. Yet, despite a long military history in the fifth domain, the economic, political, and strategic affects of cyber-attacks, and the enormous budgets to further militarise cyberspace, no act of cyber-war has *ever* taken place. All known examples of politically inspired cyber-attacks amount to either sabotage, subversion, or espionage[60], and cannot be considered *war* by the Clausewitzian[61] definition, as all three rudiments are not present: potential lethality, instrumental imposition, and perceptible political responsibility[62].

Cyber-doom and Threat Inflation

Several high-profile cases are often referenced as evidence of impending cyber-war: the Estonian and Georgian DDoS incidents; The *Operation Aurora* case in which Google, Yahoo, Symantec, Northrop Grumman, and Morgan Stanley were compromised[63]; The *Gh0stNet* espionage network which leveraged Web 2.0 and cloud-based technologies to infect embassies, foreign ministries, NGOs, and government departments, implicating a Chinese SIGINT base[64]; The *Stuxnet* sabotage of Iran's uranium enrichment facilities at Natanz, ostensibly with US and Israeli involvement; and the sophisticated espionage toolkit *Flame*[65].

The drumbeat of "cyber-doom"[66] scenarios, replayed in the media echo-chamber, has provided a steady and constant cadence for the oratory emanating from Washington and Westminster[67]. Prophetical disaster rhetoric evoked by 'expert' commentators envisage a cataclysmic cyber event, in which the financial sector collapses, planes collide midair, trains derail, military defences disintegrate, industrial control systems fail, “lethal clouds of chlorine gas” leak from chemical plants, gas pipelines and refineries explode, dams breach,

[59] *ibid.*
[60] Rid, (2012a)
[61] Clausewitz, (1832)
[62] Rid, (2012); Severs-Millard, (2012)
[63] Paul, (2010); Naraine, (2010); Severs-Millard, (2012); Clinton, (2011)
[64] Glaister, (2009); Markoff, (2009)
[65] Zetterer, (2012)
[66] Dunn-Cavelty, (2007); Dunn-Cavelty, (2008)
[67] Brito & Watkins, (2011)

reactors meltdown, power blackouts engulf the country, satellites spin into the obis, and "thousands of people" die, but authorities are impotent in the face of crumbling communications[68]. This tone continues elswhere: *Secretary of Defense*, Leon Panetta's ominous forecast of a looming "cyber Pearl Harbour", former head of the *National Cyber Security Division*, Amit Yoran's claims “cyber-9/11 has happened”, Vanity Fair's portrayal of *Stuxnet* as the "Hiroshima of cyber-war", and *Director of the International Telecommunications Union*, Hamadoun Touré's claims that "cyber-war will be worse than a tsunami", are the most infamous, vacuous, and distasteful examples of this apocalyptic theme[69]. Although the most revealing doomsday framing[70] comes from former *Senate Armed Services Committee Chairman*, Carl Levin, when he stated; "cyberweapons and cyberattacks… approach weapons of mass destruction in their effects"[71].However, nothing remotely resembling 'cyber-doom' has come to pass, and no fatality nor building destruction has even been attributable to a cyber-attack[72]. Despite Estonian politicians claiming that DDoS attacks and “a nuclear explosion…[are] the same thing”[73], NATO's *Cyber Defence Centre of Excellence* described the impact of the attacks as “minimal” or “nonexistent”[74].

Solipsistic introjection of imagined character traits onto an invisible enemy[75], combined with the technological-malaise characteristic of late-modernity[76], has seen the development of societal pessimism, dystopian fears, and sense of "political impotence" regarding the prevalence of modern technologies[77]. These fears are reminiscent of bygone anxieties regarding earlier communicative mediums and reflective of broader, tenuous concerns about societal fragility[78]. Previous 20th Century 'moral panics' over increased radio, telegraph, and telephone use, ultimately proved unfounded and transient[79].

Parallels with WMDs do, however, provide an illuminating comparison in one regard. In the run up the Iraq war the Bush administration described a "bullet-proof"[80] link between

[68] Clarke, (2010)
[69] Panetta, (2012); Gross, (2011); Schneier, (2010); Meyer, (2010)
[70] Dunn-Cavelty, (2007); Dunn-Cavelty, (2008)
[71] Levin, (2010)
[72] Rid, (2012)
[73] Poulsen, (2007)
[74] Ottis, (2010:720)
[75] Suler, (2004)
[76] Bauman, (2000)
[77] Marx, (1997:984)
[78] Crowley & Heyer, (2006)
[79] Cohen, (1972); Crowley & Heyer, (2006)
[80] Scmitt, (2002)

Sadaam Hussein and 9/11 – purportedly providing training to al-Qaeda[81]. Controlled leaks implied Iraq held WMDs, successfully conflating the very different threats of chemical, biological, and nuclear weapons[82]. Although allegations – including the purchase of 'yellowcake' for uranium enrichment – were ultimately proved fallacious, 40% of Americans still believed Saddam Hussein was "personally involved" as late as 2006[83]. Although no evidence substantiated the alarmist claims, the media relayed the government line without scrutiny[84]. It is this amplification of risk, or 'threat inflation', that Cramer and Thrall[85] describe. Unsubstantiated suppositions, such as China "lac[ing] US infrastructure with logic bombs"[86], and unverifiable assertions from the *Center for Strategic and International Studies (CSIS)* that cyber threats represent "a strategic issue on par with weapons of mass destruction and global jihad"[87], fuel cyber-doom advocacy, and conflate sabotage, espionage, and subversion, under the banner of 'cyber-war' in a manner eerily redolent of Iraq WMD threat inflation[88].

The Cyber-Industrial-Complex

President Eisenhower's 1961 farewell address warned of a "hostile ideology…global in scope, atheistic in character, ruthless in purpose"[89]. He feared deepening monetary relationships between legislators, the military, and the industry providing defence services and supplies, would lead to skewed national, economic, and security priorities, in what he phrased the "military-industrial-complex"[90]. As during the Cold War, contemporary cyber-war rhetoric maintains pressure to keep up, or fall behind, in this neoteric digital arms race[91]. Despite technical and intelligence queries as to how cyber-weapons would be deployed, the distinct absence of empirical evidence, and multifaceted ambiguities surrounding who, why, and what is under threat, and from whom[92], a thriving cyber-industrial-complex has emerged to rescue us from cyber-doom.

[81] Bush, (2002)
[82] Brito & Watkins, (2011)
[83] CNN, (2006)
[84] Massing, (2004)
[85] Crammer & Thrall, (2009)
[86] Clarke, (2010:99)
[87] CSIS, (2008: 15)
[88] Brito & Watkins, (2011)
[89] Digital History, (2012)
[90] *ibid.*
[91] Deibert, (2011)
[92] Walt, (2010); Stohl, (2007); Greenwald, (2010)

In 2010, 1,931 private companies worked on intelligence and homeland security programmes in the US, 143 were contracted to "top secret" cyber operations[93]. In an era of austerity and defence cuts, US cyber-security expenditure is predicted to rise from $9.2 billion to $14 billion by 2016[94]. The global cyber-security market, currently worth $65.7 billion, will climb to $85 billion by 2016, growing by 9% in 3 years[95]. Upward budget trajectories have galvanised the cyber-security market, where the biggest beneficiaries will be traditional defence giants such as Boeing, Lockheed Martin, Raytheon, ManTech, and Northrop Grumman, who are already repositioning themselves within the cyber-industrial-complex[96]. Leading technology companies like Symantec, IBM, Cisco, and McAfee will also prosper[97], as will smaller cyber-security start-ups like *NopSec*, whose revenue rocketed by 600% since its launch[98].

"Those who profit from war in materiel and machinery will be supplanted in time by those who profit in war from digital goods."

— Dan Geer, Chief Information Security Officer, In-Q-Tel [99]

However, it is not public-private partnerships that Eisenhower feared, but rather the deep-seated relations between policymakers, the military, and commercial venture, particularly where companies place themselves as objective experts and/or seek political "opportunity to sustain themselves"[100]. In the US, the boundaries are so porous and convoluted, that one cannot see the wood for the trees. Sen. John Rockefeller's former Chief of Staff, turned Cisco Systems cyber-security lobbyist, Jim Gottlieb, donated $19,000 the Democrat candidate[101]. Rockefeller, who famously sought retroactive immunity for AT&T's warrantless wire-tapping[102], proposed the *2010 Cybersecurity Act* which directed billions into cyber-security programmes, prompting Sen. Ron Wyden to proclaim that the US is witnessing:

[93] Priest *et al.* (2010ab)
[94] Deltek, (2011); Deibert & Rohozinski, (2011)
[95] Gartner (2012)
[96] Deibert & Rohozinski, (2011:34); Romm & Martinez, (2012); Flamm, (2013); Cole & Gorman, (2009)
[97] Ricdela, (2010)
[98] *ibid*.
[99] Grey, (2008)
[100] John Slye, *cited in* Romm & Martinez, (2012)
[101] FEC, (2013)
[102] EFF, (2005)

"The development of an industry that profits from fear … creat[ing] a cyber-industrial-complex that has an interest in preserving the problem to which it is the solution" [103]

This is indicative of the intensifying and intricate nexus of relationships developing. The election of Rep. Jim Langevin was funded primary by General Dynamics and Raytheon. Deloitte and BAE were amongst the top five contributors to Rep. Mike McCaul. Both men co-chair the CSIS panel, alongside Lt. Gen. (Ret) Harry Raduege, now IT executive for *Deloitte*, and Scott Charney, *Corporate Security Vice President* at *Microsoft*[104]. These conflicts of interest cast severe doubts over CSIS' objectivity, as well as the agendas the policies they influence may serve[105]. Inveterate relationships have also seen the revolving-door culture of employment and opportunity develop. Former *NSA Director*, Vice Adm. (Ret) Michael McConnell, became *Director of Defense* at Booz Allen Hamilton, before being reinstated as *Director of National Intelligence* by the Bush administration. McConnell then later rejoined Booz Allen as *Head of Cybersecurity Business*, prior to Booz Allen securing a $71.5 million cyber-security contract, totalling $189.4 million if extended to 2016[106]. Boeing, Lockheed Martin, and BAE have all hired ex-military or security officials in cyber-security operations[107]. In 2012 Lockheed Martin won a $400 million contract facilitating the *Pentagon's Cyber Crime Center* and Northrop Grumman secured a three-year, $189 million cyber DoD resilience contract[108].

Conclusion

Cyberspace has evolved from the auxiliary and novel, to the essential and omnipresent. Technological advancements have seen the internet develop from a research tool, to a ubiquitous framework transcending, connecting, and underpinning every facet of modern society. The post-territorial, nature of the internet has dissolved geopolitical boundaries, creating a borderless, open, but ultimately ungoverned, virtual region. The exponential rise of cyberspace within an incredibly short time frame, has meant growth has accelerated faster than government abilities to control this emerging terrain.

[103] Webster, (2012)
[104] Carney, (2011)
[105] Brito & Watkins, (2011)
[106] Mclean, (2011)
[107] Carney, (2011)
[108] Romm & Martinez, (2012)

Demographical shifts and the ascension of the global South as cyberspace's prospective new majority, have brought new cultural, social, political and strategic priorities, underscoring real-world challenges to Western hegemonic dominance. These changes have aided shifting perceptions of what 'cyberspace' entails and represents, to the point that cyberspace is viewed as a domain in its own right, comparable to land, sea, air, and space. In the past, information fluidity and system connectivity took precedence over authentication, identity, and security. Consequentially, networked systems and platforms in energy, finance, transport, and communication sectors, have seen industrial control systems, critical infrastructure, and national capabilities reliant upon networks intended to be open, collaborative, and malleable. Unsurprisingly, this has led to a dynamic, complex, and rapidly developing threat landscape, with a spectrum of attacks mounted against individuals, governments, businesses, and industries, as malicious actors seek to exploit system vulnerabilities to further their political, criminal, or nefarious ends.

Within a geostrategic paradigm, cyber-attacks have had profound effect on: economic competitiveness and the loss of national advantage; technical attribution, plausible deniability, and diplomatic accountability; and governmental attention and political oratory paid to control, and security. Collectively, these factors have successfully redefined national goals and ambitions to reflect a strategically offensive stance, with discourses now firmly framed within the language of 'pre-emptive' action to protect interests. Reinforced by government narratives, and dramatically reported by an often uninformed and sensationalist media, several high-profile incidents, of varying seriousness and sophistication, have also brought cyber-security to the forefront of public consciousness. 'Cyber-doom' scenarios and apocalyptic prophecies have become commonplace, resulting in inappropriate and inane analogies. Despite lacking empirical evidence, cyber-attacks have been placed as equivalent to humanitarian crises, natural disasters, and even nuclear war.

Threat inflation has heralded a flurry of top-down legislative and budgetary accommodations regarding cyber-security, and the establishment of many new government entities with the sole focus of achieving geostrategic ambitions. These are mainly facilitated by military and intelligence entities who have a longstanding history of operating in the cyber domain. Enormous cyber-centric budgets have resulted in a burgeoning global industry, in which companies compete for government contracts and practitioners enjoy a revolving-door of work opportunities between government, military, and private industry. Consequentially, the cyber-industrial-complex has deeply ingrained relationships, resulting

in clear conflicts of interest, and the erosion of objectivity. Individuals, companies, and governments whose business interests and careers are served by the maintenance of anxiety concerning cyber-security, convolute and inflate threats presenting their services as the solution.

Future Direction

Whilst online threats — stolen state secrets, intellectual property, competitive advantage and personal data — pose very real and difficult challenges for governments and private industry. The alarmist knee-jerk reaction to those threats and the societal fragility, the aggressive lobbying pursued, and the conflation of interests, raise serious concerns over larger, more calculated, commercial strategies and demonstrate how the cyber-industrial-complex has fanned the flames of a neoteric digital arms race.

This could result in an expensive Cold War-esque stand-off between those nation states at the forefront of the race for cyber dominance, namely America, Israel, Russia, Iran and China, escalating tensions further and eroding diplomatic and trade relations. This also risks coalescing military activity with subversion and economic espionage, subsumed under the catch-all banner of 'cyber-war'. Secondly, absorption of talent and technology within the war machine, alongside increased asymmetric tactics by malicious actors circumventing attribution, will likely spawn new white and black-hat electronic markets engaged in the pernicious trading of cyber-arms, exploits, and botnet services, as increased labour divisions result in a modular business module[109]. Moreover, the actual security benefits achieved by extensive cyber-weapon investment may prove misplaced, weighed up against astronomical development costs. Target information must be so detailed and precise, that powerful weapons will only be of use against a solitary target, and for a single assault, before exploits 'burn-out'. Furthermore, the speed technology evolves, compared to the time required to research, develop, and deploy a sophisticated cyber-weapon, means the shelf-life of weaponised code is short lived, risking weapon redundancy before deployment.

HG Wells' optimism, expressed in *The World Brain,* had been replaced by pessimism and scepticism by the time he published *Mind at the End of its Tether*. In a similar manner, fears of a dystopian dependence upon technology, as well as enduring but largely erroneous anxieties about the brittleness of contemporary society, have led to a cyber paranoia and

[109] Sageman *et al*.(2008); Rid & Mc Burney, (2012)

the merging of diagnostic and motivational discourses. The top-down militarisation of the fifth domain is hyperbolic and ineffective, discordant to the founding principles of cyberspace and at odds with prevailing W3 trends. Deterrence and protection likely to be more successful by resilience building, thorough upgrading, repairing, and modernising of systems, alongside encouraging decentralised, user-generated, organisation and governance of social arenas.

Detailed technical analysis; gauging vulnerabilities, developing technical solutions, and reconsidering software and systems architecture is critical. Adopting multi-disciplinary approaches to include analytical perspectives from political science, military and technology history, disaster sociology, and security studies, can also offer important insights, vital objectivity, and contextual grounding. This paper seeks to add to the burgeoning body of literature within this rapidly evolving field, and attempts to promote empirically grounded, research driven, and analytically sober debate with the mind to inform more conversant and commensurate cyber-security policymaking.

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]

Alexander, K. (2011) 'Building a New Command in Cyberspace'

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]

Amit, V. (2002) 'Reconceptualizing Community' in Amit, V. (Ed.) (2002) Realizing community: Concepts, Social Relationships and Sentiments, London: Routledge

Andres, R. (2013) 'Cyber-Gang Warfare: State-sponsored militias are coming to a server near you' Foreign Policy, 11th February, {Online Resource} Available at: http://www.foreignpolicy.com/articles/2013/02/11/cyber_gang_warfare?page=0,1

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]

Brito, J & Watkins, T. (2011) 'Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy', Working Paper, No.11-24, Mercatus Center, George Mason University Press, {Online Resource} Avialble at: http://mercatus.org/sites/default/files/WP1124_Loving_cyber_bomb.pdf

Byres, E & Lowe, J. (2004) 'The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems', Proceedings paper of the VDE Congress, VDE Association for Electrical Electronic and Information Technologies, October

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]

Carney, T. (2011) 'The rise of the cybersecurity-industrial complex', Washington Examiner, 27th April, {Online Resource} Available at: http://washingtonexaminer.com/carney-the-rise-of-the-cybersecurity-industrial-complex/article/113362

Cabinet Office (2011) 'The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world', November, {Online Resource}: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Cabinet Office (2012) 'The UK Cyber Security Strategy: One year on', December, {Available Resource} Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/83755/Cyber_Security_Strategy_one_year_on_achievements.pdf

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

Clinton, H. (2011) 'Internet Freedom', Internet Freedom Conference, The Hague, 8th December, {Online Resource} Available at: http://www.youtube.com/watch?v=1Lh_X-sRIVU

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

Clayton, M.(2011) 'Cyberwar timeline', The Christian Science Monitor, 11th March, {Online Resource} Available at: http://www.csmonitor.com/USA/2011/0307/Cyberwar-timeline

Cramer, J & Thrall, T (2009) 'Framing Iraq: threat inflation in the marketplace of values' American Foreign Policy and the Politics of Fear 174

Cole, A. & Gorman, S. (2009) 'Defense Firms Pursue Cyber-Security Work' The Wall Street Journal, 18th March

Crowley, D. & Heyer, P. (2006) 'Communication in History: Technology, Culture, Society' Boston:Pearson, 210-216

CSIS Commission(2008) 'Securing Cyberspace for the 44th Presidency: CSIS Commission Report on Cybersecurity for the 44th Presidency', December, {Online Resource} Available at: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Czosseck, C., Ottis, R. & Talihärm, AM. (2011) 'Estonia After the 2007 Cyber Attacks: Legal, Strategic & Organisational Changes in Cyber Security' International Journal of Cyber Warfare and Terrorism, 1(1): 24-34, January-March, {Online Resource} Available: http://www.irma-international.org/viewtitle/61328/

Deibert, R. & Rohozinski, R. (2011a) 'The new cyber military-industrial complex', Citizen Lab, 28th March {Online Resource} Available at: https://citizenlab.org/2011/03/deibert-and-rohozinski-the-new-cyber-military-industrial-complex/

Deibert, R. & Rohozinski, R. (2011b) 'Contesting Cyberspace and the Coming Crisis of Authority' in Access Contested: Security, Identity, and Resistance in Asian Cyberspace, MIT Press (Eds) Palfrey, J. Rohozinski, R. & Zittrain, J. {Online resource} Available http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-chapter-02.pdf [Accesses 08/02/13]

Deibert, R. & Rohozinski, R. (2008) 'Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet' In Access Denied: The Practice and Policy of Global Internet Filtering (Eds) Deibert R., Palfrey, J., Rohozinski, R., Zittrain, J. MIT Press. {Onlne Resource} avaible at: http://opennet.net/sites/opennet.net/files/Deibert_07_Ch06_123-150.pdf

Deibert, R. (2011a) 'Tracking the emerging arms race in cyberspace, Bulletin of the Atomic Scientists, 67(1):1-8

Deibert, R. (2011b) 'The rise of Asian cyberspace: Challenges and opportunities for Canada' Asia Pacific Foundation, 12th September

Deibert, R. (2012) 'Towards Stewardship in Cyberspace' The G8 Research Group, 18th May, {Online Resource} Available at:http://citizenlab.org/wp-content/uploads/2012/05/g8campdavid2012-04-36.pdf

Deibert, R. & Crete-Nishihata, M. (2012) 'Global Governance and the Spread of Cyberspace Controls," in Global Governance: A Review of Multilateralism and International Organizations', 18(3):339-361, {Online Resource} Available at: http://citizenlab.org/cybernorms2012/governance.pdf

Deltek (2011) 'Agile Business Intelligence: Or how to win in the 21st century business climate' {Online Resource} Available at: http://more.deltek.com/forms/Agile-Business-Intelligence-White-Paper

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]

Department of Defense (2012a) 'Sustaining U.S. Global Leadership: Priorities for 21st Century', U.S Government, {Online Resource} Available at: http://www.defense.gov/news/defense_strategic_guidance.pdf

Department of Defense (2012b) 'The Federal Budget: Fiscal Year 2012', Office of Management and Budget,{Online Resource} Available at: http://www.whitehouse.gov/omb/factsheet_department_defense

Department of Defense (2012c) 'The Federal Budget: Fiscal Year 2013', Pg72-84, Office of Management and Budget,{Online Resource} Available at: http://www.whitehouse.gov/sites/default/files/omb/budget/fy2013/assets/defense.pdf

Digital History (2012) 'The Military-Industrial Complex' Digital History ID 3409, http://www.digitalhistory.uh.edu/disp_textbook.cfm?smtID=2&psid=3409

Dunn-Cavelty, M. (2008) 'Cyber-Terror: Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate', Journal of Information Technology & Politics, 4(1): 19-36 {Online Resource} Available at: http://www.tandfonline.com/doi/pdf/10.1300/J516v04n01_03

Dunn-Cavelty, M. (2007) 'Cyber-Security and Threat Politics: US Efforts to Secure the Information Age', London: Routledge

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

Electronic Frontier Foundation (2005)'Case M-06-cv-01791-VRW: NSA of the Southwest, Inc, et al', NSA Telecommunications Records Litigation, United States District Court for the Northern District of California {Online Resource} Available at: https://www.eff.org/files/filenode/att/orderhepting6309_0.pdf

Federal Election Commission (2013) 'Disclosure Data Search: Candidate and Committee Viewer' {Online Resource} Available at: http://www.fec.gov/finance/disclosure/disclosure_data_search.shtml

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

Flamm, M.(2013) 'A paranoia industrial complex emerges', Crain's New York Business, 17th February, {Online Resource} Available at: http://www.crainsnewyork.com/article/20130217/TECHNOLOGY/302179976

Gartner (2012) 'Gartner's Agenda for Government 2013' {Online Resource} Available at: http://www.gartner.com/technology/research/content/government-public-sector.jsp

Gasparre, R. (2008a) 'The Israeli 'E-tack' on Syria: Part One' {Online Resource} Available at: http://www.airforce-technology.com/features/feature1625

Gasparre, R. (2008b) 'The Israeli 'E-tack' on Syria: Part Two' {Online Resource} Available at: http://www.airforce-technology.com/features/feature1669

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

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

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

Grey, P. (2008) 'Risky Business #83 - The Military Digital Complex: Interview with Dan Geer'', Risky Business, http://risky.biz/netcasts/risky-business/risky-business-83-military-digital-complex

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]=

Gjelten, T (2011) 'Seeing the Internet as an Information Weapon', National Public Radio, September 23rd, {Online Resource} Available at: http://www.npr.org/templates/story/story.php?storyId=130052701&sc=fb&cc=fp {Accessed 08/02/2013]

Glenny, M. (2010) 'States embark on a scramble for cyberspace', Financial Times, 18th March, {Online Resource} Available at: http://www.ft.com/cms/s/0/220d70d4-322d-11df-b4e2-00144feabdc0.html#axzz2LXTFoGpU

Greene, T., James, L. & Strawn, G. (2003) 'A Brief History of NSF and the Internet'. National Science Foundation, {Online Resource} Available at: http://www.nsf.gov/od/lpa/news/03/fsnsf_internet.htm

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]

Hilbert, M. & López, P. (2011) 'The World's Technological Capacity to Store, Communicate, and Compute Information', Science Journal, 332(6025): 60-65 {Online resource} Available at: http://www.sciencemag.org/content/332/6025/60 [Accesses 08/02/13]

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]

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]

Internet World Statistics (2010a) 'World Internet Usage and Population Statistics' {Online Resource} Available at: http://www.internetworldstats.com/stats.htm

Internet World Stats (2010b) 'The Internet Big Picture: World Internet Users and Population Stats' {Online Resource} Available at: http://www.internetworldstats.com/stats.htm

International Telecommunication Union (2010) 'ITU Estimates Two Billion People Online by End 2010' 19th October, {Online Resource} Available at: http://www.itu.int/net/pressoffi ce/press_releases/2010/39.aspx

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

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]

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

Lawson, S. (2011) 'Beyong Cyber Doom: Cyberattack Scenarios and the Evidence of History'Working Paper, No.11-24, Mercatus Center, George Mason University Press

Levin, C. (2010) 'Introductory Speech', 111th United States Senate Armed Services Committee, Webcast. {Online Resource} Available at: http://www.armed-services.senate.gov/Webcasts/2010/04%20April/04-15-10%20Webcast.htm

Lord, K. & Sharp, T. et al. (2011) 'America's Cyber Future: Security and Prosperity in the Information Age', Center for a New America Security, June, Vol 2. {Online Resource} Available at: http://www.cnas.org/files/documents/publications/CNAS_Cyber_Volume%20II_2.pdf

Lynn, WJ. (2011) 'The Pentagon's Cyberstrategy, One Year Later Defending Against the Next Cyberattack' September 2011, {Online Resource} Avialable at: http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later?page=show

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]

Massing, M. (2004) 'Now They Tell Us: the American Press and Iraq'. New York: New York Review of Books

Marx, L. (1997) 'Technology: The Emergence of a Dangerous Concept' Social Research 64(3):965-988

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]

Mclean, VA.(2011) 'Booz Allen Hamilton gets Naval cybersecurity deal', Bloomberg Businessweek, 20th April, {Online Resource} Available at: http://www.businessweek.com/ap/financialnews/D9MNI3EO0.htm

NATO (2010) 'Active Engagement, Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation", Lisbon Sumit, {Online Resource} Available at: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

Ottis, R. (2010) 'The Vulnerability of the Information Society', FutureGOV Asia Pacific, August-September, 7(4):70-72 {Online Resource} Available at http://www.futuregov.asia/media/downloads/Magazine_7_4.pdf

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]

Poggi, G (2006) 'Weber: A Short Introduction', Cambridge: Polity

Priest, D. et al (2010a) 'Top Secret America: The Top Secret Network of Governmetn and its Contractors', Washington Post, {Online Resource} Available at: http://projects.washingtonpost.com/top-secret-america/network/#/single/gov-orgs/socom/

Priest, D. et al (2010b) 'Top Secret America: Cyber Operations', Washington Post, {Online Resource} Available at:http://projects.washingtonpost.com/top-secret-america/functions/cyber-ops

Poulsen, K. (2007) 'Cyberwar and Estonia's Panic Attack', Threat Level, 22nd August, {Online Resource} Available at: http://www.wired.com/threatlevel/2007/08/cyber-war-and-e.

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]

Rosenberg, B. (2012) 'Winners and losers in the fiscal 2013 budget', Defense Systems, March, {Online Resource} Available at: http://defensesystems.com/Articles/2012/02/28/Editors-Note-fiscal-2013-defense-budget-analysis.aspx?Page=1

Roberts, M.(2012) 'DHS breaks down 2013 cybersecurity budget', 12th March, {Online Resource} Available at: http://urgentcomm.com/policy-amp-law/dhs-breaks-down-2013-cybersecurity-budget

Romm, T. & Martinez, J. (2012) 'Cyberthreats turn into megabucks for defense companies', PoliticoPro, 30th May, http://www.politico.com/news/stories/0512/76841_Page2.html

Ricdela, A. (2010) 'Symantec, McAfee, Checkpoint Await Spending Surge' Bloomberg Businessweek, 18th Jan, {Online Resource} Available at: at:http://www.businessweek.com/print/technology/content/jan2010/tc20100115_453540.htm

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

Rid, T. & Mc Burney, P. (2012) 'Cyber-Weapons' RUSI Journal, Feburary/March 157(1):6–13 {Online Resource} Available at: http://www.rusi.org/downloads/assets/201202_Rid_and_McBurney.pdf

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

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

Sangani, K. (2011) 'Sony Security Laid Bare' Engineering & Technology Journal, 6(8):74-77

Schreier, J (2011) 'Sony Estimates $171 Million Loss From PSN Hack', May, {Online Resource} Available at: http://www.wired.com/gamelife/2011/05/sony-psn-hack-losses/

Schneier, B (2010) 'Threat of 'cyberwar' has been hugely hyped', CNN, 7th July, {Online Resource} Available at: http://edition.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/index.html

Severs, H. (2012a) 'Surfing the Jihadisphere: how the internet facilites violent radicalisation', The Risky Shift, {Online Resource} Available at: http://theriskyshift.com/2012/05/essay-internet-and-violent-html/ [Accessed 20/11/12]

Severs, H. (2012b) 'Lessons from Dayr-az-Zawr' {Online Resource} Available at: http://theriskyshift.com/2012/10/syria-cyberwarfare-lessons-from-dayr-az-zawr/

Severs, H. (2012c) 'The Greatest Transfer of Wealth in History: How significant is the cyber espionage threat', The Risky Shift, {Online Resource} Available at: http://theriskyshift.com/2013/01/cyber-espionage-the-greatest-transfer-of-wealth-in-history/ [Accessed 20/11/12]

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

Sokolski, H. (2012) 'The Next Arms Race', Strategic Studies Institute, US Army War College, {Online Resource} Available at:http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1113.pdf

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]

Stohl, M. (2007) 'Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point Or Patriot Games?', Crime, Law and Social Change, 46(4-5):223-238

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]

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

United Nations Office of High Representative for Least Developed Countries, Landlocked Developing Countries and Small Island Developing States (2010) 'Least Developed Countries: About LDCs' {Online Resource} Avialble at: http://www.unohrlls.org/en/ldc/25

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]

Walt, SM. (2010) 'Is the Cyber Threat Overblown?', Foreign Policy, 30th March, {Online Resource} Available at: http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown.

Webster, S. (2012) 'Sen. Wyden: CISPA creates a Cyber Industrial Complex to feed on private data', RawStory, 22nd May, {Online Resource} Available at: http://www.rawstory.com/rs/2012/05/22/sen-wyden-cispa-creates-cyber-industrial-complex-to-feed-on-private-data

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]