# Weber HT---NDT Rd 1 vs Wayne State JS

## 1AC

### 1AC---Chaos

#### In the aftermath of 9-11, preemption logic has proliferated, vindicating all action in the face of radical uncertainty

Stockdale, 13

(Liam Stockdale, Ph.D. in International Relations, Department of Political Science, McMaster University. “Imagined Futures and exceptional presents: a conceptual critique of ‘pre-emptive security’” <http://www.tandfonline.com/doi/abs/10.1080/14781158.2013.774342>) Henge

A growing body of work has meticulously documented the emergence of pre-emption as a prominent security rationality in the post-9/11 era.11 While addressing a wide range of practices — including, but not limited to, the indefinite detention,12 extraordinary rendition,13 and targeted killing14 of suspected terrorists; the widespread biometric monitoring of increasingly mobile populations;15 the pre-emptive detention of refugees and asylum seekers;16 the anticipatory freezing of monies and assets suspected of terrorist ties;17 and the so-called ‘Bush Doctrine’ of pre-emptive interstate war18 — this burgeoning literature has collectively highlighted the importance of temporally inflected, future-oriented strategies in the global security climate. The following discussion seeks to both tie together and build upon this literature’s insights, so as to move toward a comprehensive conceptual account of pre-emptive security as it has (re-)emerged in the contemporary context. I hope also to begin to demonstrate how this emergent ‘primacy of pre-emption’19 entails significant, and potentially problematic, implications for the way political power is exercised with respect to questions of (in)security — a point which will be considered in greater detail in the next section. To begin, it is useful to consider how and why the logic of pre-emption has come to dominate the post-9/11 global security climate. The key point here is that its rise has been largely coeval with the emergence of transnational terrorism as the dominant issue. This is because in the aftermath of the 9/11 attacks, which the prevailing narrative cast as an out-of-the blue evental irruption,20 the specific security problem of terrorism became identified with the broader existential problem of temporal uncertainty.21 From the outset, therefore, the post-9/11 governance of (in) security was effectively ‘temporalized’, as the terroristic event was framed as ultimately ‘unpredictable in occurrence, characteristics, and effects’.22 Importantly, such a characterization rendered conventional security logics such as deterrence or containment largely inapplicable in the context of terrorism, since these are essentially ineffective in circumstances where the threat in question is defined by its radical incalculability.23 The global security environment thus became increasingly framed in terms reminiscent of Ulrich Beck’s ‘risk society’ thesis,24 with established practical certainties and techniques of control appearing to break down in the face of apparently novel threats.25 Political authorities thus became ‘much less certain of whether and when they [were] secure, and how - and to what extent and at what price — security [could] be achieved’,26 and terms such as ‘extreme uncertainty’,27 ‘radical contingency’,28 and other such expressions of perniciously excessive ambiguity came to pervade accounts of the global security environment. However, it is in precisely such a context that the logic of pre-emption proves compelling, since it explicitly delineates a programme for action that actively confronts uncertainty by ostensibly enabling decision-makers ‘to counter the unknowable before it is even realized’.29 Since the spectre of terrorism in particular appears to require precisely such a capability if it is to be governed,30 the proliferation of pre-emptive strategies, mechanisms, and technologies of security has been a central feature of the post-9/ 11 global security climate — to the extent that one commentator has aptly referred to the latter as a ‘state of pre-emption’.31 The logic of pre-emption as manifested in the security strategies of the post-9/11 era is thus best understood as a political rationality that allows action to be taken in the face of apparent radical uncertainty. Normatively speaking, it is premised upon mitigating the potentially pernicious effects of that uncertainty by (re-)asserting control over the unfolding of the future through anticipatory interventions in the present. Yet because the future can never be known absolutely, a certain ‘objective uncertainty’ is at the core of the logic of preemption.32 As a result, the decisional rationality of pre-emption differs markedly from other logics of political decision-making. Indeed, more conventional logics such as rational calculation and cost—benefit analysis — as well as other, more temporally inflected security logics such as deterrence and prevention — all assume at least some degree of certainty with respect to the substantive basis for action.33 This is not to imply that these decisional logics require complete knowledge and/or total certainty; but rather that they are generally premised upon inductive processes and rooted in the use of verifiable knowledge to develop actionable assumptions with a certain degree of empirically rooted confidence. This diverges importantly from the logic of pre-emption, which takes radical uncertainty precisely as its departure point, as the mere potential of future danger provides the basis for anticipatory intervention in the present. This location of radical uncertainty at the core of the logic of pre-emption thus gives its decisional rationality a highly speculative character. The potential futures against which pre-emptive decisions are framed possess no ontological presence apart from their existence in the realm of the speculative. It is therefore not verifiable empirical fact that forms the primary basis of a preemptive decision, but conjectural articulations of potential (and potentially dangerous) futures.34 As Claudia Aradau and Rens van Munster put it, ‘what counts is a coherent scenario of catastrophic risk and an imaginary description of the future’.35 Accordingly, a pre-emptive security decision is effectively freed from any necessary link to verifiable knowledge or empirical fact.36 Rather, decision-makers are encouraged ‘to take into account doubtful hypotheses and simple suspicions to take the most far-fetched forecasts seriously’, since the Cartesian ‘malicious demon’ of catastrophe might emerge at any time.37 Through its ‘appropriation of uncertainty as the basis for action’ rather than an impediment to action,38 pre-emptive security thus creates a political climate in which decision-makers are induced to ‘break free from the “tyranny” of [the] plausible’.39 Indeed, the indefinite future is precisely that which is being acted upon; and so any necessary tie to empirical fact would too heavily constrain the scope of decisional possibility, since no such ‘facts’ exist in relation to a future that exists beyond the realm of the wholly knowable. The logic of pre-emptive security thus resembles the so-called ‘precautionary principle’ more familiar to theories of environmental governance, as the evidentiary circumscriptions of the decisional process are diminished considerably.40 Of course, preemptive decisions do not necessarily constitute entirely arbitrary exercises in speculation — although they can manifest as such. The point is rather that the role of the speculative and the conjectural is significantly higher than is the case under other political rationalities. In fact it must be, since the logic of pre-emption seeks to act upon a future that necessarily remains ulti— mately unknowable and thus ‘beyond the horizon of certainty’.41 This reliance on speculative and conjectural knowledge suggests that there are significant political implications to adopting a pre-emptive approach to (in)security governance. In particular, it implies that a pre—emptive politics of security hinges on the exercise of the imagination by relevant decision-makers, since this is the only way politically actionable ‘knowledge’ about the ultimately unknowable future can be generated. The next section explores the implications of this point in greater detail, and specifically considers how such a prioritization of the imagination suggests a crucial conceptual link between the logic of pre-emptive security and the logic of political exceptionalism.

#### Status quo offensive cyber ops are a fear-driven militarization of the cyber realm---the cyber-industrial complex hypes cyber-threats for profit, causing a self-fulfilling prophecy

Severs, 13

(Henry Severs holds 1st (Hons) in Criminology & Social Policy from the University of Sheffield, further awarded the Vaughan Bevan Prize by the Faculty of Law. Currently a postgraduate of War Studies at King's College London, reading Terrorism, Security, & Society as a Stapley Trust Scholar. “The Cyber-Industrial-Complex” <http://theriskyshift.com/2013/03/the-cyber-industrial-complex-2/>) Henge

This paper lays plain the growing pressure and increased enthusiasm of governments, armed services, and commercial actors to develop and operationalise military capabilities in cyberspace. The argument shall be made that the lines between these ostensibly distinct spheres have become increasingly muddied, and we are witnessing the emergence of a new cyber-industrial-complex. Furthermore, ~~blind~~ [misplaced] faith that the militarisation of the fifth domain will achieve effectual cyber security is misplaced and, ultimately, the top-down control of cyberspace — at odds with prevailing internet behaviour — is an expensive means to achieve relatively ineffectual security. Reference will be made to relevant case studies and conceptual frameworks from the social sciences. Analysis is approached through five convergent lines of enquiry: To provide context, first the development of the internet from a ‘tool’ to a ‘territory’ shall be discussed; exploring the various technological, demographic, and social shifts this evolution has fostered. Next, the geostrategic impact of cyber threats shall be touched upon, describing the economic, legal and strategic affects profoundly influencing our 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’. Following on, a discussion of ‘threat inflation’ and ’cyber-doom’ narratives shall be presented, critiquing parallels drawn between ‘cyber-war’ and Weapons of Mass Destruction (WMDs). Finally, the amalgamation of political, military, and commercial interests within the ‘cyber-industrial-complex’ shall be examined. In concluding, many of the challenges facing policymakers will be considered, and the call for sober, research-driven policy prescriptions will again be reiterated. Primarily however, the inherent limitations of exploring a relatively young, multidisciplinary field examining such a rapidly evolving subject must be acknowledged[1]. Themes discussed here are therefore more akin to Weberian concepts of ideal typical discourses than static social truths[2]. Despite this papers validity and current application, it is but a cursory examination of the cyber-industrial-complex, intended to stimulate further debate, and as such caution should be exercised when making wider generalisations, predications or forecasts[3]. Indeed, it is suggested that the hyperbolic status quo should be reflected upon, reconsidered, and replaced with a far more objective risk assessment of the threats posed. In order to effectively address the question and avoid tangential theoretical debates, the utility of explicitly expressed working definitions is crucial — appreciating that more appropriate vernacular may very well 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]. The World Brain: from Tool to Territory To contextualise changing attitudes and perceptions of 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 the Defense Advanced Research Projects Agency (DARPA), envisioned a ‘Galactic Network’ of globally connected computers through which anyone could access information. Advancements in packet switching, standardisation of Internet protocols, and the expanded connection of the original ARPANET to include research and education institutions in the 1970/80s, saw 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]. 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 global 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~~ [expansion] 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 some of 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, 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 the virtual arena who would otherwise be 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 simply a medium, or even 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 attracted 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 their 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 territory[28]. Minimal barriers and relative anonymity of malicious actors, combined with the emergence of Web 2.0 and “malware ecosystems” propagating hacking tool-kits and botnets, have allowed determined groups — whether criminals, freelancers, military 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 networks, infrastructure, and communications[30]. Within a geostrategic paradigm, such threats have profoundly influenced the militarisation of cyberspace[31]: Firstly, there is 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 warning letters to the top 300 British businesses stressing the threat of “electronic espionage”[40]. Although ascribing the true cost of cyber-attacks is extremely difficult, immeasurable even, it is clear the costs from intellectual property and R&D theft alone are enormous, rising, and potentially of the magnitude to influence global power relations[41]. Secondly, we see an obscurity of political liability by utilising proxy servers, ‘cyber-militias’, and freelance hackers to execute attacks [42]. Potentially creating the smoke and mirrors useful for implanting ‘logic bombs’ into critical infrastructure, but primarily affording states plausible deniability for actions likely at odds with their 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 any serious diplomatic repercussions, essentially punishing Estonia whilst circumventing legal accountability for targeting civilian institutions[45]. In more 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 radar images to display 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 and markets to this end. Militarising the Fifth Domain The four year, £650m British Cyber Security Strategy emphasises protective, defensive, and ‘pre-emptive’ action aimed at: 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 stated goals[50]. It details numerous provisions seeking 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 — a necessary and welcomed development — the offensive stance throughout is arrant: “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] 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 now 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 the unprecedented tri-hatting of Gen. Keith Alexander as Director of NSA, Chief of the Central Security Service, and Commander of USCYBERCOM. In the 2013 US fiscal budget cyber capabilities are a priority; 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 will be spent 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 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 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: violence and potential lethality of the act, instrumental imposition will over another, and perceptible and attributable 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 networks 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 military SIGINT base and organised crime[64]; The Stuxnet sabotage of Iran’s uranium enrichment facilities at Natanz, seemingly 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 Westminster and especially Washington[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, reactors meltdown, power blackouts engulf the country, satellites spin into the obis, and “thousands of people” die… but authorities are paralysed in the face of crumbling communications and digital devastation[68]. This tone continues elsewhere: 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]. Yet, 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] This solipsistic introjection – assigning imagined behaviours and character traits onto an invisible enemy[75] – combined with a technological malaise characteristic of late-modernity[76], has seen the development of societal pessimism, dystopian fears, and a 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, soon to be surpassed by the latest technological trepidation[79] The WMD parallel does, 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 Sadaam Hussein and 9/11 – purportedly providing refuge and training to al-Qaeda[81]. Controlled Whitehouse leaks implied Iraq held WMDs, successfully conflating the very different threats and consequences 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” in 9/11 as late as 2006[83]. Although no evidence substantiated these alarmist claims, the media relayed the government line without scrutiny and the administration was essentially able to cite news articles written speculating upon their own fictitious leaks[84]. It is this amplification of risk, or ‘threat inflation’, that Cramer and Thrall[85] describe. Speculative commentary about Iranian or North Korean cyber capabilities, unsubstantiated suppositions of the Chinese “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 the neoteric digital arms race[91]. Despite technical and intelligence ambiguities as to how cyber-weapons would actually 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 save us from our cyber-doom. 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 an extraordinary 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 has rocketed by 600% since its recent 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, for the CIA’s 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, these boundaries are now 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: “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]. Too Fast to Tie Down 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 ability to control this emerging terrain. 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 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.

#### This threat perception is flawed---Cold War fears have spilled over to cyberspace and the military lashes out for lack of control

Cavelty, 12

(Dr. Myriam Dunn Cavelty is Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich, Switzerland and was Fellow at the “stiftung neue verantwortung” in Berlin, Germany. She publishes regularly in international journals and has authored and edited several books on information age security issues In addition to her teaching, research and publishing activities, she advises governments, international institutions and companies in the areas of cyber security, cyber warfare, critical infrastructure protection, risk analysis and strategic foresight. As an internationally renowned cyber expert she is a frequent speaker at professional conferences. “The militarisation of cyber security as a source of global tension” <http://ssrn.com/abstract=2007043>) Henge

Over the last few years, cyber security has been catapulted from the confined realm of technical experts into the political limelight. The discovery of the industry-sabotaging Stuxnet computer worm, numerous tales of (Chinese) cyber espionage, the growing sophistication of cyber criminals, and the well-publicised activities of hacker collectives have combined to give the impression that cyber attacks are becoming more frequent, more organised, more costly, and altogether more dangerous. As a result, a growing number of countries consider cyber security to be one of the top security issues of the future. This is just the latest ‘surge’ of attention in the three- to four-decade-long history of cyber issues. The importance attached to cyber security in politics grew steadily in response to a continual parade of incidents such as computer viruses, data theft, and other penetrations of networked computer systems, which, combined with heightening media attention, created the feeling that the level of cyber insecurity was on the rise. As a result, the debate spread in two directions: upwards, from the expert level to executive decision-makers and politicians; and horizontally, advancing from mainly being an issue of relevance to the US to the top of the threat list of more and more countries. The debate on ‘cyber security’ originated in the US in the 1970s, built momentum in the late 1980s, and spread to other countries in the late 1990s. Early on, US policy-makers politicised the issue. They presented cyber security as a matter that requires the attention of state actors because it cannot be solved by market forces. As concern increased, they securitised the issue: They represented it as a challenge requiring the urgent attention of the national security apparatus. In 2010, against the background of the Stuxnet incident, the tone and intensity of the debate changed even further: The latest trend is to frame cyber security as a strategic-military issue and to focus on countermeasures such as cyber offence and defence, or cyber deterrence. Though this trend can easily be understood when considering the political (and psychological) effects of Stuxnet, it nonetheless invokes images of a supposed adversary even though there is no identifiable enemy, is too strongly focused on national security measures instead of economic and business solutions, and wrongly suggests that states can establish control over cyberspace. Not only does this create an unnecessary atmosphere of insecurity and tension in the international system, it is also based on a severe misperception of the nature and level of cyber risk and on the feasibility of different protection measures. While it is undisputed that the cyber dimension will play a substantial role in future conflicts of all grades and shades, threat-representations must remain well informed and well balanced at all times in order to rule out policy reactions with excessively high costs and uncertain benefits. This chapter first describes the core elements of the cyber security debate that emerged over the past decades. These elements provide the stage and scenery for the more recent trend of increasing militarisation of cyber security. Five factors responsible for this trend are described in section two. The effects of the discovery of Stuxnet as the culmination point of the cyber threat story are the focus of section three: Though the actual (physical) damage of Stuxnet remains limited, it had very real and irreversible political effects. The fourth section critically assesses the assumptions underlying the trend of militarisation and their negative effects. The chapter concludes by arguing that military countermeasures will not be able to play a significant role in cyber security due to the nature of the information environment and the nature of the threat. Finally, it sketches the specific, though limited role that military apparatuses can and should play in reducing the overall level of cyber insecurity nationally and internationally. The backdrop of the cyber security debate The combination of telecommunications with computers in the late 1970s and the 1980s – the basis of the current information revolution – marks the beginning of the cyber threat debate. The launch and subsequent spread of the personal computer created a rise in tech-savvy individuals, some of whom started to use the novel networked environment for various sorts of misdeeds. In the 1990s, the information domain became a force multiplier by combining the risks to cyberspace (widespread vulnerabilities in the information infrastructure) with the possibility of risks through cyberspace (actors exploiting these vulnerabilities). The two core elements of the cyber security debate that provide the stable backdrop for the current trend of militarisation emerged: A main focus on highly vulnerable critical infrastructures as ‘referent object’ (that which is seen in need of protection) and the threat representation based on the inherent insecurity of the information infrastructure and the way it could be manipulated by technologically skilful individuals. From government networks to critical infrastructures Initially, the overarching concern of the US was with the classified information residing in government information systems. As computer networks grew and spread into more and more aspects of everyday life, this focus changed. A link was established in the strategic community between cyber threats and so-called ‘critical infrastructures’, which is the name given to assets whose incapacitation or destruction could have a debilitating impact on the national security and/ or economic and social welfare of the entire nation. This threat perception was influenced by the larger strategic context that emerged for the US after the Cold War. It was characterised by more dynamic geostrategic conditions, more numerous areas and issues of concern, and smaller, more agile, and more diverse adversaries. As a result of the difficulties to locate and identify enemies, the focus of security policies partly shifted away from actors, capabilities, and motivations to general vulnerabilities of the entire society. In addition, the influence of globalisation on the complex interdependence of societies around the world and their growing technological sophistication led to a focus on security problems of a transnational and/or technological nature. The combination of vulnerabilities, technology, and transnational issues brought critical infrastructures to centre stage, particularly because they were becoming increasingly dependent on the smooth functioning of all sorts of computer-related applications, such as software-based control systems. The basic nature of the cyber threat The networked information environment – or cyberspace – is pervasively insecure, because it was never built with security in mind. The dynamic globalisation of information services in connection with technological innovation led to a steady increase of connectivity and complexity. The more complex an IT system is, the more problems it contains and the harder it is to control or manage its security. The commercialisation of the Internet led to an even further security deficit, as there are significant marketdriven obstacles to IT security. These increasingly complex and global information networks seemed to make it much easier to attack the US asymmetrically: Potentially devastating attacks now only required a computer with an Internet connection and a handful of ‘hackers’, members of a distinct social group (or subculture) who are particularly skilled programmers or technical experts. In the borderless environment of cyberspace, hackers can exploit computer insecurities in various ways. In particular, digitally stored information can be delayed, disrupted, corrupted, destroyed, stolen, or modified. Intruders can also leave ‘backdoors’ to come back at a later time, or use the hijacked machine for attacks on other machines. Though most individuals would be expected to lack the motivation to cause violence or severe economic or social harm, large sums of money might sway them to place their specialised knowledge at the disposal of actors with hostile intent like terrorists or foreign states. In addition, attackers have little to fear in terms of retribution. Sophisticated cyber attacks cannot be attributed to a particular perpetrator, particularly not within a short timespan. The main reasons are the often hidden nature of exploits and the general architecture of cyberspace, which allows online identities to be hidden. Five developments that speed up militarisation The basics as described above provided a stable setting for the cyber security debate at least since the mid-1990s, if not before. Five developments as described below have solidified the impression that cyber disturbances are increasingly dangerous and fall under the purview of national security. The discovery of Stuxnet is the culmination point in this evolution. It has brought about a qualitative and irreversible change in how the issue is handled politically: Its discovery has catapulted the cyber issue from the expert level to the diplomatic and foreign policy realm. First, computer security professionals are increasingly concerned with the rising level of professionalisation coupled with the obvious criminal (or even strategic) intent behind attacks. Tech-savvy individuals (often juveniles) aiming to create mischief or personally enrich themselves shaped the early history of computer-related crime. Today, professionals dominate the field. Actors in the ‘cyber crime black market’ are highly organised in terms of their strategic and operational vision, logistics, and deployment. Like many legitimate companies, they operate across the globe. As a consequence, the nature of malware has changed. Advanced malware is targeted: A hacker picks a victim, examines the defences, and then designs specific malware to get around them. The most prominent example for this kind of malware is Stuxnet (see below). Second, the main cyber ‘enemy’ in the form of a state has been singled out: There is an increase in allegations that China is responsible for cyber espionage in the form of high-level penetrations of government and business computer systems, in Europe, North America, and Asia. Because Chinese authorities have stated repeatedly that they consider cyberspace a strategic domain and that they hope that mastering it will equalise the existing military imbalance between China and the US more quickly (see Chapter 1 in this publication), many US officials readily accuse the Chinese government of perpetrating deliberate and targeted attacks or intelligence-gathering operations. However, because of the attribution problem, these allegations almost exclusively rely on anecdotal and circumstantial evidence. Not only can attackers hide, it is also impossible to know an attacker’s motivation or to know a person’s affiliation or sponsorship, even if the individuals were known. Therefore, attacks and exploits that seemingly benefit states might well be the work of third-party actors operating under a variety of motivations. At the same time, the attribution challenge also conveniently allows state actors to distance themselves officially from attacks.

#### Fears of proliferation are misplaced---cyber codes become obsolete before they can be utilized more than once

Cavelty, 12

(Dr. Myriam Dunn Cavelty is Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich, Switzerland and was Fellow at the “stiftung neue verantwortung” in Berlin, Germany. She publishes regularly in international journals and has authored and edited several books on information age security issues In addition to her teaching, research and publishing activities, she advises governments, international institutions and companies in the areas of cyber security, cyber warfare, critical infrastructure protection, risk analysis and strategic foresight. As an internationally renowned cyber expert she is a frequent speaker at professional conferences. “The militarisation of cyber security as a source of global tension” <http://ssrn.com/abstract=2007043>) Henge

In the mainstream representation of the Stuxnet story, the Bushehr nuclear plant is the intended target of the attack. Indeed, the operational start of Bushehr was delayed by several months: Iranian officials blamed the hot weather and later a leak for it. Officially, Tehran at first denied the worm infected critical systems at the Bushehr plant, but later said that Stuxnet had affected a limited number of centrifuges. There also seemed to have been some problems at Natanz: A decline in the number of operating centrifuges from mid-2009 to mid-2010 may have been due to the Stuxnet attack, some experts speculate. All in all, knowing the extent of the effect Stuxnet had on the Iranian nuclear programme is impossible; it seems plausible, however, that is has delayed it, though only for a short amount of time. The psychological effect on the Iranian government, though also not easily fathomable, is likely to have been very high. Proliferation effect The discovery of Stuxnet and subsequent rumours that its source code was for sale led some experts to fear a rapid proliferation of this type of programming and many so-called piggyback attacks. This would make SCADA systems – computer systems that monitor and control industrial, infrastructure, or facility-based processes – the target of choice in the near to mid-term future for all types of hacks, with potentially grave consequences, also due to unintended side effects. Other analysts have described these fears as groundless, because even if somebody had acquired the source code, they would have to be just as capable as the initial programmers for the variant to be as successful. Once a piece of malware has been discovered, even if it is a sophisticated specimen, merely copying it will be of little use if the computer vulnerability it exploited has been patched in the meantime. So far, no proliferation effect has materialised; however, in September 2011, another worm (Duqu) was discovered that is reportedly very similar to Stuxnet, and was probably written by the same authors. It mainly looks for information that could be useful in attacking industrial control systems and does not sabotage any parts of the infrastructure. Political and psychological effect The greatest effect the worm has had is clearly psychological: It has left many state officials deeply frightened. This fear has political consequences. First, on the national level, governments are currently releasing or updating cyber security strategies and are setting up new organisational units for cyber defence. Second, internationally, increased attention is being devoted to the strategic-military aspects of the problem. The focus is on attacks that could cause catastrophic incidents involving critical infrastructures. More and more states report that they have opened ‘cyber-commands’, which are military units for cyber war activities. Though consolidated numbers are hard to come by, the amount of money spent on defence-related aspects of cyber security seems to be rising steadily. The new cyber military-industrial complex that has emerged is estimated to deliver returns of US$ 80 to 150 billion a year, and big defence companies like Boeing and Northrop Grumman are repositioning themselves to service the cyber security market. In addition, some states, particularly those not allied with the US, have ramped up their rhetoric. For example, Iranian officials have gone on the record as condoning hackers who work in the state’s interest. As a result, the first signs of a cyber security dilemma are discernible: Although most states still predominantly focus on cyber defence issues, measures taken by some nations are seen by others as covert signs of aggression. That leads to more insecurity for everyone – specifically because it is impossible to assess another state’s cyber capabilities. Flawed assumptions and detrimental effects The militarisation of cyber security is first and foremost based on the belief in a massive threat of a large-scale cyber attack. There are two aspects to this perception: In the first subsection, it is shown how and why the past and current level of the threat is overrated. The second subsection places the future likelihood of cyber war into perspective. It shows that now and in the future, the probability of a large-scale attack is very low. The third subsection looks at an additional reason for how widespread the fear of cyber war has become: Most countries simply follow the threat perception and reasoning of the US, even though the strategic context and disparity in power positions warrant a different threat assessment. The fourth subsection finally criticises the widespread use of vocabulary that is full of military analogies. Such vocabulary insinuates a reality governed by the traditional logic of offense and defence – a reality that does not exist. Even worse, it is decoupled from the reality of the threat and the possibility for meaningful countermeasures and is complicit in solidifying the militarisation of cyber security. An overrated threat There is no denying that different political, economic, and military conflicts have had cyber(ed) components for a number of years now. Furthermore, criminal and espionage activities involving the use of computers happen every day. It is a fact that cyber incidents are continually causing minor and only occasionally major inconveniences: These may be in the form of lost intellectual property or other proprietary data, maintenance and repair, lost revenue, and increased security costs. Beyond the direct impact, badly handled cyber attacks have also damaged corporate (and government) reputations and have, theoretically at least, the potential to reduce public confidence in the security of Internet transactions and e-commerce if they become more frequent. However, in the entire history of computer networks, there are no examples of cyber attacks that resulted in actual physical violence against persons (nobody has ever died from a cyber incident), and only very few had a substantial effect on property (Stuxnet being the most prominent). So far, cyber attacks have not caused serious long-term disruptions. They are risks that can be dealt with by individual entities using standard information security measures, and their overall costs remain low in comparison to other risk categories such as financial risks. These facts tend to be almost completely disregarded in policy circles. There are several reasons why the threat is overrated. First, as combating cyber threats has become a highly politicised issue, official statements about the level of threat must also be seen in the context of competition for resources and influence between various bureaucratic entities. This is usually done by stating an urgent need for action and describing the overall threat as big and rising. Second, psychological research has shown that risk perception, including the perception of experts, is highly dependent on intuition and emotions. Cyber risks, especially in their more extreme form, fit the risk profile of so-called ‘dread risks’, which are perceived as catastrophic, fatal, unknown, and basically uncontrollable. There is a propensity to be disproportionally afraid of these risks despite their low probability, which translates into pressure for regulatory action of all sorts and the willingness to bear high costs of uncertain benefit. Third, the media distorts the threat perception even further. There is no hard data for the assumption that the level of cyber risks is actually rising – beyond the perception of impact and fear. Some IT security companies have recently warned against overemphasising sophisticated attacks just because we hear more about them. In 2010, only about 3 per cent of all incidents were considered so sophisticated that they were impossible to stop. The vast majority of attackers go after low-hanging fruit, which are small to medium sized enterprises with bad defences. These types of incidents tend to remain under the radar of the media and even law enforcement. Cyber war remains unlikely Since the potentially devastating effects of cyber attacks are so scary, the temptation is very high not only to think about worst-case scenarios, but also to give them a lot of (often too much) weight despite their very low probability. However, most experts agree that strategic cyber war remains highly unlikely in the foreseeable future, mainly due to the uncertain results such a war would bring, the lack of motivation on the part of the possible combatants, and their shared inability to defend against counterattacks. Indeed, it is hard to see how cyber attacks could ever become truly effective for military purposes: It is exceptionally difficult to take down multiple, specific targets and keep them down over time. The key difficulty is proper reconnaissance and targeting, as well as the need to deal with a variety of diverse systems and be ready for countermoves from your adversary. Furthermore, nobody can be truly interested in allowing the unfettered proliferation and use of cyber war tools, least of all the countries with the offensive lead in this domain. Quite to the contrary, strong arguments can be made that the world’s big powers have an overall strategic interest in developing and accepting internationally agreed norms on cyber war, and in creating agreements that might pertain to the development, distribution, and deployment of cyber weapons or to their use (though the effectiveness of such norms must remain doubtful). The most obvious reason is that the countries that are currently openly discussing the use of cyber war tools are precisely the ones that are the most vulnerable to cyber warfare attacks due to their high dependency on information infrastructure. The features of the emerging information environment make it extremely unlikely that any but the most limited and tactically oriented instances of computer attacks could be contained. More likely, computer attacks could ‘blow back’ through the interdependencies that are such an essential feature of the environment. Even relatively harmless viruses and worms would cause considerable random disruption to businesses, governments, and consumers. This risk would most likely weigh much heavier than the uncertain benefits to be gained from cyber war activities. Certainly, thinking about (and planning for) worst-case scenarios is a legitimate task of the national security apparatus. Also, it seems almost inevitable that until cyber war is proven to be ineffective or forbidden, states and non-state actors who have the ability to develop cyber weapons will try to do so, because they appear cost-effective, more stealthy, and less risky than other forms of armed conflict. However, cyber war should not receive too much attention at the expense of more plausible and possible cyber problems. Using too many resources for highimpact, low-probability events – and therefore having less resources for the low to middle impact and high probability events – does not make sense, neither politically, nor strategically and certainly not when applying a cost-benefit logic. Europe is not the US The cyber security discourse is American in origin and American in the making: At all times, the US government shaped both the threat perception and the envisaged countermeasures. Interestingly enough, there are almost no variations to be found in other countries’ cyber threat discussions – even though the strategic contexts differ fundamentally. Many of the assumptions at the heart of the cyber security debate are shaped by the fears of a military and political superpower. The US eyes the cyber capabilities of its traditional rivals, the rising power of China and the declining power of Russia, with particular suspicion. This follows a conventional strategic logic: The main question is whether the cyber dimension could suddenly tip the scales of power against the US or have a negative effect on its ability to project power anywhere and anytime. In addition, due to its exposure in world politics and its military engagements, the US is a prime target for asymmetric attack. The surely correct assumption that modern societies and their armed forces depend on the smooth functioning of information and communication technology does not automatically mean that this dependence will be exploited – particularly not for the majority of states in Europe. The existence of the cyber realm seems to lead people to assume that because they have vulnerabilities, they will be exploited. But in security and defence matters, careful threat assessments need to be made. Such assessments require that the following question be carefully deliberated: ‘Who has an interest in attacking us and the capability to do so, and why would they?’ For many democratic states, particularly in Europe, the risk of outright war has moved far to the background and the tasks of their armies have been adapted to this. Fears of asymmetric attacks also rank low. The same logic applies to the cyber domain. The risk of a warlike cyber attack of severe proportions is minimal; there is no plausible scenario for it. Cyber crime and cyber espionage, both political and economic, are a different story: They are here now and will remain the biggest cyber risks in the future. The limits of analogies Even if the cyber threat were to be considered very high, the current trend conjures up wrong images. Analogies are very useful for relating non-familiar concepts or complex ideas with more simple and familiar ones. But when taken too far, or even taken for real, they begin to have detrimental effects. Military terms like ‘cyber weapons’, ‘cyber capabilities’, ‘cyber offence’, ‘cyber defence’, and ‘cyber deterrence’ suggest that cyberspace can and should be handled as an operational domain of warfare like land, sea, air, and outer space (cyberspace has in fact been officially recognised as a new domain in US military doctrine). Again, this assumption clashes with the reality of the threat and the possibilities for countermeasures. First, calling offensive measures cyber weapons does not change the fact that hacker tools are not really like physical weapons. They are opportunistic and aimed at outsmarting the technical defences. As a result, their effect is usually not controllable in a military sense – they might deliver something useful or they might not. Also, even though code can be copied, the knowledge and preparation behind it cannot be easily proliferated. Each new weapon needs to be tailored to the system it is supposed to attack. Cyber weapons cannot be kept in a ‘silo’ for a long time, because at any time, the vulnerability in the system that it is targeted at could be patched and the weapon would be rendered useless. Second, thinking in terms of attacks and defence creates a wrong image of immediacy of cause and effect. However, high-level cyber attacks against infrastructure targets will likely be the culmination of long-term, subtle, systematic intrusions. The preparatory phase could take place over several years. When – or rather if – an intrusion is detected, it is often impossible to determine whether it was an act of vandalism, computer crime, terrorism, foreign intelligence activity, or some form of strategic military attack. The only way to determine the source, nature, and scope of the incident is to investigate it. This again might take years, with highly uncertain results. The military notion of striking back is therefore useless in most cases. Third, deterrence works if one party is able to successfully convey to an- other that it is both capable and willing to use a set of available (often military) instruments against the other side if the latter steps over the line. This requires an opponent that is clearly identifiable as an attacker and has to fear retaliation – which is not the case in cyber security because of the attribution problem. Attribution of blame on the basis of the cui bono logic is not sufficient proof for political action. Therefore, deterrence and retribution do not work in cyberspace and will not, unless its rules are changed in substantial ways, with highly uncertain benefits. Much of what is said in China and in the US about their own and the other’s cyber capabilities is (old) deterrence rhetoric – and must be understood as such. The White House’s new International Strategy for Cyberspace of 2011 states that the US reserves the right to retaliate to hostile acts in cyberspace with military force. This ‘hack us and we might bomb you’ statement is an old-fashioned declaratory policy that preserves the option of asymmetrical response as a means of deterrence, even though both sides actually know that following up on it is next to impossible. Fourth, cyberspace is only in parts controlled or controllable by state actors. At least in the case of democracies, power in this domain is in the hands of private actors, especially the business sector. Much of the expertise and many of the resources required for taking better protective measures are located outside governments. The military – or any other state entity for that matter – does not own critical (information) infrastructures and has no direct access to them. Protecting them as a military mandate is impossible, and conceiving of cyberspace as an occupation zone is an illusion. Militaries cannot defend the cyberspace of their country – it is not a space where troops and tanks can be deployed, because the logic of national boundaries does not apply. The role of the military in cyber security Future conflicts between nations will most certainly have a cyberspace component, but this will just be an accompanying element of the battle. Regardless of how high we judge the risk of a large-scale cyber attack, military-type countermeasures will not be able to play a substantial role in cyber security because of the nature of the attacker and the nature of the attacked. Investing too much time talking about them or spending increasing amounts of money on them will not make cyberspace more secure – quite the contrary. These findings are not particularly new: Most experts had come to the same conclusion in the late 1990s, when the debate was not yet as securitised. At the time, the issue was discussed under the heading of critical infrastructure protection rather than cyber security, but the basic premises were the same. The role for the military as conceptualised then hardly differs from the role the military should take on today. Undoubtedly, attacks on information technology, manipulation of information, or espionage can have serious effects on the present and/or future of defensive or offensive effectiveness of one’s own armed forces. First and foremost, militaries should therefore focus on the protection and resilience of their information infrastructure and networks, particularly the critical parts of it, at all times. All the successful attacks on military and military-affiliated networks over the last few years are less a sign of impending cyber-doom than a sign of low information security prowess in the military. In case the unfortunate label ‘cyber defence’ should stick, it will be crucial to make sure that everybody – including top-level decisionmakers – understand that cyber defence is not much more than a fancy word for standard information assurance and risk management practices. Furthermore, information assurance is not provided by obscure ‘cyber commands’, but by computer security specialists, whether they wear uniforms or not. The cyber dimension is also relevant in military operations insofar as an adversary’s critical infrastructure is deemed to be a major centre of gravity, i.e., a source of strength and power that needs to be weakened in order to prevail. However, intelligence-gathering by means of cyber espionage must be treated with utmost care: In an atmosphere fraught with tension, such activities, even if or especially because they are non-attributable, will be read as signs of aggression and will add further twists to the spiral of insecurity, with detrimental effects for everybody. The implication of this is that military staff involved in operative and military strategic planning and the intelligence community will have to be aware of cyber issues too. However, in the future, decisive strikes against critical (information) infrastructure will most likely still consist of kinetic attacks or traditional forms of sabotage rather than the intrusion of computer systems. As for the things the military should not do when it comes to the realm of cyberspace, two major points come to mind. First, particularly as long as the ability to withstand cyber intrusions of military networks or civilian networks remains low, it is unwise to declare the development or possession of offensive measures. It does not have a credible deterring effect, the actual use would bring unclear benefits and high risks, and again, it adds to the cyber security dilemma.

#### Cyber threat reps are a set of discursive constructions---rhetoric of cyber war is formulated to exacerbate fears and threaten the order of law

Cavelty, 13

(Dr. Myriam Dunn Cavelty is Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich, Switzerland and was Fellow at the “stiftung neue verantwortung” in Berlin, Germany. She publishes regularly in international journals and has authored and edited several books on information age security issues In addition to her teaching, research and publishing activities, she advises governments, international institutions and companies in the areas of cyber security, cyber warfare, critical infrastructure protection, risk analysis and strategic foresight. As an internationally renowned cyber expert she is a frequent speaker at professional conferences. “From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse” doi: 10.1111/misr.12023) Henge

Cyber-Threat Representations: Creating and Changing “the Reservoir” Cyber-security as understood in this paper is a combination of linguistic and non-linguistic discursive practices from many different “communities” of actors. To systematize threat representations, this diversity needs to be mapped.5 While the common topic in all communities is the security of computers and computer networks, they differ most in their focus on the type of issues on a higher level, which they regard as being connected to or influenced by the security of computers and computer networks. In other words, the biggest difference between the communities is the “referent object” to which they pay particular attention. Taking these different referent objects in the broader discourse as the basis for the mapping, four clusters can be formed: In each cluster, particular groups of actors are shaping and driving the discourse, and there are specific threats to the referent objects they are concerned about (Table 1). Table 1 reveals considerable overlap with regard to the threats discussed in each cluster. A combination of the most similar types leads to three clusters of threat types: The first is technical in nature, focusing on malware (a portmanteau word combining “malicious” and “software”). The second is about socio- political threats, mainly human “wrongdoers” in a variety of shapes. The third is focused on human–machine interactions (Table 2). When looking more closely at these threat types, particular ways of talking about these threats become obvious: These “ways of talking” are the threat representations this paper is interested in.6 The technical domain is particularly rich in biological, and particularly virus-related, metaphors. The second capitalizes on the lawlessness of cyberspace (or the Western Frontier) and mainly revolves around shady, invisible, but powerful foes. The third is focused on the complex- ity of the computer infrastructure and the societal vulnerabilities created by our dependency on the computer infrastructure. These three threat types with their particular threat representations, including their origins and evolution, are detailed below in three subsections. These three influence countermeasures and form “the reservoir” on which visible political actors draw, as will be shown in the next section. Biologizing Technology: Viruses, Worms, and Other Bugs The first threat representation is about “digital accidents” (Sampson 2007) in the form of malware and the biological register employed for their depiction. The concept of the information virus was, like cyberspace, coined in sci-fi literature, 7 but it took a computer scientist rather than an activist to popularize it (Parikka 2007). Fred Cohen’s experiments with self-replicating mini-programs in the 1980s mark an important milestone in the conceptualization of software as risk. His description of the (substantial) danger stemming from computer viruses uses the image of a biological killer virus: As an analogy to a computer virus, consider a biological disease that is 100% infectious, spreads whenever animals communicate, kills all infected animals instantly at a given moment, and has no detectable side effects until that moment. […] If a computer virus of this type could spread throughout the computers of the world, it would […] wreak havoc on modern government, financial, business, and academic institutions. [Cohen 1987] When home computers and with them viral metaphors became more widespread in the 1980s, they were vivid and effective ways of explaining to non-technical experts how malware works and were actively used as such by computer specialists.8 However, a real-world incident and a lot of media attention were needed to instill in the public mind the imagery of (digital) viruses. The “Morris Worm” was such an incident. The worm used so many system resources that the attacked computers could no longer function and large parts of the early Internet went down (Parrika 2005). Thereafter, the image of computers as the epitome of control, reliability, efficiency, and order was transformed into an image of computers as threatened by the unexpected, though inevitable danger of rogue, rampant programs. Professional and popular discussions of computer viruses figured computer systems as self-contained bodies that must be protected from outside threat. These discussions mainly fed on anxieties about sexual contamination in populations, particularly AIDS, as expressed in statements like “Browsing the Internet without protection is just plain foolish!,”9 or calling behavioral computer rules “safe hex” practices. Computer security rhetoric about compromised networks also employs language suggestive of that used to describe the bodies of nation-states under military threat (Lupton 1994). Such language describes viruses using images of foreignness, illegality, and otherness. The biological description of viruses as key “intruder technology” is militarized: A virus consists of self-replicating code and a “payload.” The former is like the propulsion unit of a missile; the latter is the warhead it delivers (Helmreich 2000:473). The use of science-fiction terminology as the main source of cyber-threat representations in the technological domain seems an inevitable consequence of both the closeness of the computer community to the sci-fi subculture and a lack of alternatives. When the Internet and computer networks began to spread, there were few literary realms other than sci-fi with its fascination for outer space and alien life forms that could have helped policymakers and the public to learn how to cope with these novelties. Given the special place viruses have in history as one of the scourges of mankind, fear from infectious disease, virtual or real, is deeply ingrained in the human psyche, so that employing viral metaphors for things we are scared of, especially “known unknowns,” seems to come naturally to us.10 The parallels between “real” biological viruses (and the discourses about them) and its digital variants are striking. Not only have biological metaphors directly inspired technical innovation (like genetic algorithms or evolutionary programming), but biological models have also led creative individuals to new and more disruptive ways of programming malware (like polymorphic code that mutates). Also, biology occasionally looks to computer viruses to learn about viral and societal behavior, as in the case of the “Corrupted Blood” incident in “World of Warcraft” (Balicer 2005). This virtual plague, which was due to a programming error, “mirrored real-world epidemics in numerous ways: It originated in a remote, uninhabited region and was carried by travelers to urban centers; hosts were both human and animal, such as with avian flu; it was spread by close spatial contact” (Orland 2008). Most importantly, however, when looking at the evolution of the technical threat representations, AIDS has stopped being the prime health concern in the Western world—our epidemic fears today revolve around viruses that jump boundaries, especially those that overcome species barriers (zoonotics), like Swine Flu or Ebola. In 2010, the computer world had its own barrier-jumping incident, when a worm known as Stuxnet overcame the barrier between the virtual and the corporeal worlds by having a “real” (opposed to virtual) effect. Stuxnet was discovered in June 2010 and has been called “[O]ne of the great technical blockbusters in malware history” (Gross 2011) due to its complexity and sophistication. While it was initially impossible to know for certain who was behind this piece of code, though many suspected one or several state actors (Farwell and Rohozinski 2011), it was revealed in mid-2012 that Stuxnet is part of a US and Israeli intelligence operation, programmed and released to sabotage the Iranian nuclear program. For many observers, Stuxnet as a “digital first strike” marks the beginning of an age of (unrestrained) cyber-war between states. In the post-Stuxnet world, viruses are no longer like the common flu—they have killer qualities. Like the virus bred in the bio-terrorists’ laboratory, the modern computer virus is increasingly conceptualized as a weapon, aimed at a specific target. And where there is a weapon, there is malicious intent, which is where the second type of threat representation comes in. Anonymous Data Wizards in Lawless Space Socio-political threats and their representations do not thrive on metaphors much. Rather, the material realities of computer networks and malicious activities taking place in or through them that manifest as “digital accidents” shape the threat representations in this cluster. New categories of threats were formed in government circles and think-tanks by linking the prefix “cyber-” to estab- lished and known threats to security, thus creating terms such as cyber-vandalism, cyber-crime, cyber-espionage, cyber-terror, or cyber-war (Denning 2012). “Old” forms of deviant behavior become “new” as they are imbued with a sense of “through the use of a computer” or “related to cyberspace.” The exact origin of these terms is sometimes hard to fathom, and tracking down the provenance for individual terms would be a lengthy undertaking; what seems most relevant in the context of this article is that behind all of these categories is in essence the archetype/stereotype of the “hacker,” individuals with technical superpowers. In the early stages of the discourse, computer hackers were depicted as highly skilled (male) youths (Ross 1991). Once again, it was popular culture that was at the forefront of shaping the simplified image of “the hacker.” The movie War Games (1983) in particular is regarded as crucial for not only giving substance to the hacker culture, but also for exposing the general public to the idea of computer hacking for the first time. In this film, a young computer whizz kid sees an advert for online war games and starts trying to hack into the company’s server. When he finally gets access, he starts to play a simulated game called “global thermonuclear war”—unfortunately, he has hacked into the military simulation computer at the Pentagon, which starts to act out a response to an attack from Russia. In the end, World War III is barely averted. The popular conception of the hacker as adolescent boy, hunched over his computer and posing a latent, but severe threat to national security, was both reflected in and popularized by this movie, and supported at the same time by real-world hacking incidents. Very soon thereafter, computer hackers were increasingly branded as criminals in government circles, not least because computer break-ins seemed to become more widespread, and received a lot of media attention. In the 1980s, growing parts of society in the United States had already become dependent on computing for business practices and other basic functions. Tampering with computers suddenly meant potentially endangering people’s careers and property, and some even said their lives (Spafford 1989). Not surprisingly, the development of legal tools to prosecute unauthorized entry into computer systems (like the Computer Fraud and Abuse Act of 1986 in the United States) coincided with the first serious network incidents. Furthermore, the new “authoritative voice” in the field, the anti-virus industry, invested a great deal of resources into spreading public information about the danger from hackers (Skibell 2002). However, the evolution of the hacker image did not stop at criminalization. In general, the debate moved away from hacker criminals to terrorist hackers after 9/11 (Bendrath, Eriksson, and Giacomello 2007), and then, in parallel to the development shown in the technological cluster, on to highly professional state-sponsored cyber-mercenaries, able to develop highly effective cyber-weapons. Such conceptions are supported by reports from anti-virus companies, which describe the main threat as one from increasingly organized professionals (cf. Panda Security 2010). Over the years, this discourse has become particularly focused on so-called advanced persistent threats, a cyber-attack category that connotes an attack with a high degree of sophistication and stealthiness over a prolonged duration of time. The attack objectives typically extend beyond immediate financial gain, so that states as instigators of cyber-misdemeanor, currently mainly in the form of cyber-espionage, are the main focus of attention.

#### OCO’s are an attempt to control cyberspace, the most complex of all realms

Paganini, 13

(Pierluigi Paganini, Editor-in-Chief at Cyber Defense Magazine. “Does the US really think to leverage preemptive cyber attacks as a deterrent?” <http://www.cyberdefensemagazine.com/are-us-really-thinking-to-preemptive-cyber-attacks-as-deterrent/>) Henge

There are a great number of activities in cyber space, whereby governments are secretly conducting a huge quantity of cyber operations, and every day we read about malicious code used to steal sensible information or about cyber attacks that targeted critical infrastructures. The principal questions raised by so fervent activities are the rules of engagement and proportionality of the defense, which is the operative limit of countries that discover an attack against its networks? Is it thinkable to assume the introduction of machines in the decision-making process of defense? Recently many cases have highlighted an intense cyber espionage activity against US Governments and private industries having the principal intent to steal sensible information, the principal suspect is of course the China due the characteristic techniques adopted by the hackers. Obviously this is just the tip of the iceberg and same US are also very active in the cyberspace, but recently the Obama administration’s finding that the president has the power to order a preemptive cyber attacks to discourage those who violate the networks of the country, in particular to Chinese government which remains unresponsive to U.S. efforts to mitigate the cyber offensives originated from the country. Last Sunday The New York Times published and interesting article on the possibility that President Obama could order a strike to respond to imminent cyber threats against national critical infrastructures. The measure is limited to Homeland security menaced by threats that affect assets critical for the country and does not cover attacks on private industry like cyber espionage. “New policies will also govern how the intelligence agencies can carry out searches of faraway computer networks for signs of potential attacks on the United States and, if the president approves, attack adversaries by injecting them with destructive code — even if there is no declared war.” The alert level is increased after the recent attacks to media agencies, continuous intrusions appear originated from countries and security experts are convinced that they are state-sponsored operations due the means and methods adopted. The discussion on a possible preemptive attacks is in my opinion a provocation, it’s clear that that both US and China are pursuing their cyber strategies and are respectively conscious of the cyber capabilities of their adversaries, the declarations are a public admission of failure of diplomatic efforts spent by the governments, nothing more. It’s clear that US could increase pressure on China requiring for example major purchases of Chinese goods go through national security reviews, according to the Council on Foreign Relations (CFR), but is very different from the organization of a cyber attacks for demonstrative purpose. Is Obama’s administration really willing to give up so prolific commercial relationship? “Adam Segal wrote in a blog post that China has responded by saying through the People’s Daily that the administration’s position could trigger a worldwide arms race.” The U.S. threat of a pre-emptive strike difficultly will discourage foreign governments, contrary it could increase risk overall, many other governments could be interested to induce to think that the attacks come from China or from other hostile nations, in these case the preemptively attack could be addressed against the wrong targets due the difficulty to localize the real identity of the attackers. We must also consider that governments will continue to operate secretly in cyber space also on the offensive front, that statements of a pre-emptive attack are only a warning to the world that is intended to alert on the cyber capabilities of the country. Why take the paternity of a pre-emptive strike when nations attack today in absolute silence? Cyber weaponry is the most complex arms race under way, US government has promoted the born of a new Cyber Command, and many other governments are spending similar effort, declaration of preemptive cyber attack are useless but while a lot of words are spent on what constitutes reasonable and proportionate use of cyber force, cyber arms all over the world are sharpening their weapons. A cyber war is much more subtle and dangerous than preemptive cyber attack!

#### Therefore, Jordan and I affirm the chaos of cyberspace

#### The Socratic reason of the world is rooted in distaste for tragedy and a fear of instability---the attempt to create constancy and resolve universal contradiction only internalizes suffering and ressentiment

Saurette ‘96 [Paul, 1996 “I mistrust all Systematizers and Avoid Them: Nietzsche, Arendt and the Crisis of the Will to Order in International Relations Theory.” Millenium Journal of International Studies. Vol. 25, number 1. pp. 3-6]

The Philosophical Foundation of the Will to Truth/Order: ‘I mistrust all systematizers and avoid them. A will to a system is a lack of integrity.’ According to Nietzsche, the philosophical foundation of a society is the set of ideas which give meaning to the phenomenon of human existence within a given cultural framework. As one manifestation of the Will to Power, this will to meaning fundamentally influences the social and political organisation of a particular community. Anything less than a profound historical interrogation of the most basic philosophical foundations of our civilization, then, misconceives the origins of values which we take to be intrinsic and natural. Nietzsche suggests, therefore, that to understand the development of our modern conception of society and politics, we must reconsider the crucial influence of the Platonic formulation of Socratic thought. Nietzsche claims that pre-Socratic Greece based its philosophical justification of life on heroic myths which honoured tragedy and competition. Life was understood as a contest in which both the joyful and ordered (Apollonian) and chaotic and suffering (Dionysian) aspects of life were accepted and affirmed as inescapable aspects of human existence. However, this incarnation of the will to power as tragedy weakened, and became unable to sustain meaning in Greek life. Greek myths no longer instilled the self-respect and self-control that had upheld the pre-Socratic social order. ‘Everywhere the instincts were in anarchy; everywhere people were but five steps from excess: the monstruin in animo was a universal danger’. No longer willing to accept the tragic hardness and self-mastery of pre-Socratic myth, Greek thought yielded to decadence, a search for a new social foundation which would soften the tragedy of life, while still giving meaning to existence. In this context, Socrates’ thought became paramount. In the words of Nietzsche, Socrates saw behind his aristocratic Athenians; he grasped that his case, the idiosyncrasy of his case, was no longer exceptional. The same kind of degeneration was everywhere silently preparing itself the old Athens was coming to an end. And Socrates understood that the world had need of him —his expedient, his cure and his personal art of self-preservation. Socrates realised that his search for an ultimate and eternal intellectual standard paralleled the widespread yearning for assurance and stability within society. His expedient, his cure? An alternative will to power. An alternate foundation that promised mastery and control, not through acceptance of the tragic life, but through the disavowal of the instinctual, the contingent, and the problematic. In response to the failing power of its foundational myths, Greece tried to renounce the very experience that had given rise to tragedy by retreating/escaping into the Apollonian world promised by Socratic reason. In Nietzsche’s words, ‘[r]ationality was divined as a saviour... it was their last expedient. The fanaticism with which the whole of Greek thought throws itself at rationality betrays a state of emergency: one was in peril, one had only one choice: either to perish, or be absurdly rational...’ Thus, Socrates codified the wider fear of instability into an intellectual framework. The Socratic Will to Truth is characterised by the attempt to understand and order life rationally by renouncing the Dionysian elements of existence and privileging an idealised Apollonian order. As life is inescapably comprised of both order and disorder, however, the promise of control through Socratic reason is only possible by creating a ‘Real World’ of eternal and meaningful forms, in opposition to an ‘Apparent World’ of transitory physical existence. Suffering and contingency is contained within the Apparent World, disparaged, devalued, and ignored in relation to the ideal order of the Real World. Essential to the Socratic Will to Truth, then, is the fundamental contradiction between the experience of Dionysian suffering in the Apparent World and the idealised order of the Real World. According to Nietzsche, this dichotomised model led to the emergence of a uniquely ‘modern” understanding of life which could only view suffering as the result of the imperfection of the Apparent World, This outlook created a modem notion of responsibility in which the Dionysian elements of life could be understood only as a phenomenon for which someone, or something, is to blame. Nietzsche terms this philosophically-induced condition ressentiment, and argues that it signaled a potential crisis of the Will to Truth by exposing the central contradiction of the Socratic resolution. This contradiction, however, was resolved historically through the aggressive universalisation of the Socratic ideal by Christianity. According to Nietzsche, ascetic Christianity exacerbated the Socratic dichotomisation by employing the Apparent World as the responsible agent against which the ressentiment of life could be turned. Blame for suffering fell on individuals within the Apparent World, precisely because they did not live up to God, the Truth, and the Real World. As Nietzsche wrote, ‘I suffer: someone must be to blame for it’ thinks every sickly sheep. But his shepherd, the ascetic priest tells him: ‘Quite so my sheep someone must be to blame for it: but you yourself are this someone, you alone are to blame for yourself,—you alone are to blame for yourself—This is brazen and false enough: but one thing is achieved by it, the direction of ressentiment is altered.’Faced with the collapse of the Socratic resolution and the prospect of meaninglessness, once again, ‘one was in peril, one had only one choice: either to perish, or be absurdly rational....” The genius of the ascetic ideal was that it preserved the meaning of the Socratic Will to Power as Will to Truth by extrapolating ad absurdium the Socratic division through the redirection of ressentiment against the Apparent World! Through this redirection, the Real World was transformed from a transcendental world of philosophical escape into a model towards which the Apparent World actively aspired, always blaming its contradictory experiences on its own imperfect knowledge and action. This subtle transformation of the relationship between the dichotomised worlds creates the Will to Order as the defining characteristic of the modern Will to Truth. Unable to accept the Dionysian suffering inherent in the Apparent World, the ascetic ressentiment desperately searches for ‘the hypnotic sense of nothingness, the repose of deepest sleep, in short absence of suffering’.’3 According to the ascetic model, however, this escape is possible only when the Apparent World perfectly duplicates the Real World, The Will to Order, then, is the aggressive need increasingly to order the Apparent World in line with the precepts of the moral Truth of the Real World. The ressentiment, of the Will to Order, therefore, generates two interrelated reactions. First, ressentiment engenders a need actively to mould the Apparent World in accordance with the dictates of the ideal, Apollonian Real World. In order to achieve this, however, the ascetic ideal also asserts that a ‘truer’, more complete knowledge of the Real World must be established, creating an ever-increasing Will to Truth. This self- perpetuating movement creates an interpretative structure within which everything must be understood and ordered in relation to the ascetic Truth of the Real World. As Nietzsche suggests, “[t]he ascetic ideal has a goal—this goal is so universal that all other interests of human existence seem, when compared with it, petty and narrow; it interprets epochs, nations, and men inexorably with a view to this one goal; it permits no other interpretation, no other goal; it rejects, denies, affirms and sanctions solely from the point of view of its interpretation.’

#### The vicious ressentiment of counterterror preemption obliterates all of life’s value

Siemens and Shapiro in 2008

(Herman, Assistant Professor for the Institute for Philosophy at the University of Leiden, and Gary, Professor of Philosophy at the University of Richmond, “What Does Nietzsche Mean for Contemporary Politics and Political Thought?”, The Journal of Nietzsche Studies, Issue 35/36, Spring/Autumn, pMUSE, rcheek)

Does Fukuyama offer a genuine alternative on the questions of the “one” and the “direction of the earth”—or does the “end of history” thesis fall under Nietzsche’s geophilosophical critique of modernist, Eurocentric metanarratives issuing in technocratic utopias? There are certainly reasons for reading the end of history as a triumphalist metanarrative that advances the hegemony of the last man—in spite of Fukuyama. A good deal depends on what we make of the resources he locates and mobilizes against the narrative of the last man. Do they represent an alternative, a real source of resistance, or just an endless repetition of the fully functionalized worker/consumer? Fukuyama’s exemplars of megalothymia seem to be not only “tame,” as Sheikh concedes, but radically impoverished in comparison with Nietzsche’s “higher men” or “good Europeans,” whose signature features are hybridity, (inner and outer) multiplicity, and mobility. More importantly, Fukuyama’s identification of liberal democracy as a site of isothymia looks like wishful thinking when set against Nietzsche’s strongest formulations of contemporary nihilism. In an important Nachlass note Nietzsche argues that under modern economic-technological conditions of exploitation, human life suffers an overall loss of value, worth, or quality: “der Mensch wird geringer” (KSA 12:10[17]). The loss of commanding and sense-giving powers that accompanies the democratic processes of “contraction” and “leveling” signifies a value reduction (Werth-Verringerung) of the human type, that is, a loss of intrinsic human value or worth. Clearly, this thesis undermines the conditions for isothymia, understood as mutual recognition of intrinsic worth. If nihilism signifies this loss of intrinsic human value or worth for Nietzsche, its sources lie in a problem of the will—the loss of commanding and sense-giving powers. The thymiotic accounts of the last man and the correctives proposed by Fukuyama seem to overlook this problem completely. As Sheikh remarks in closing, the question of nihilism is the battleground for the endgame between Fukuyama and Nietzsche.¶ Tracy Strong’s article articulates the deep structure of Nietzsche’s political thought by exploring the connections of tyranny, tragedy, and philosophy. If philosophy is itself a tyrannizing force by imposing its meanings on the world and blinding itself to the limits of this imposition, then tragedy can balance this tendency by disclosing the impossibility of the tyrannical project, whether [End Page 6] political or philosophical. Strong shows how Nietzsche’s diagnosis of modernity is about a world in which tragedy is no longer part of the public sphere (itself a replacement for the agon of tyranny, tragedy, and philosophy). If tragedy is a way of fending off tyranny, Socratic rationalism, which constitutes tragedy’s death and rules in its aftermath, opens the door once more to the pursuit of a total explanation, in other words, to the search for the tyrant. Thus, the modern world sets itself up for a succession of tyrannical projects. Confirmation of Strong’s assessment of George W. Bush as a tyrant can be found in current U.S. policy of preemptive war as a new realization of the tyrannical fixation of meaning. The view that war is justified as the elimination of threats that might materialize in the future, of virtual or possible threats, presupposes a strange sense of the future as already visible. The future that preemption fears or anticipates may be brought into existence by the act of preemption itself in Iraq; preemptive war creates its own evidence by assembling terrorists enabled by a “war on terrorism.” Here we might be reminded of the ironic relation that the Greeks saw between tyrants and oracles (consider the stories of Herodotus as a commentary on the uses of “intelligence”). Thinking they knew the future, tyrants and despots launched disastrous wars and occupations in which they were both protagonist and victim. As Strong emphasizes in an allegorical reading of John Ford’s The Man Who Shot Liberty Valance and in his remarks on the current Bush presidency, the project of overcoming tyranny requires a renewed sense of community tempered by tragic wisdom.¶ In “The Innocence of Victimhood Versus the ‘Innocence of Becoming’: Nietzsche, 9/11, and the ‘Falling Man,’” Joanne Faulkner takes up the question of agency that Strong invites when he closes his essay by saying, “[t]hat murder is not possible does not mean that we must be helpless.” Faulkner argues that the hegemonic first-person post–9/11 narrative in the United States revolves around the concept of a victimized innocence, a self-image that is then used to support projects of revenge (however arbitrary and costly in life and treasure) and accepts the authority of a state of exception wherein real liberties are sacrificed for promised security. Why, she asks, were images of those who fell or jumped from the Twin Towers quickly suppressed in the media? Because, she answers, they could be read as exhibiting a moment of decision and the possibility of agency even in the most desperate and limited circumstances. The jumpers complicate the image of innocence and victimhood. Faulkner interprets the dominant U.S. narrative in terms of Nietzsche’s theory of ressentiment; if we are innocent victims, then we gladly seek revenge by ceding our powers to a higher authority. Nietzsche’s alternative concept of the Unschuld des Werdens suggests the possibility of acting outside the cycle of debt and guilt. Here innocence—Unschuld—is understood as freedom from that kind of moral thinking; accepting the innocence of becoming is “integral to the skillful exercise of agency” and [End Page 7] to making “a choice to take part in the inevitability of the moment.” Faulkner shows how Nietzsche’s thought on agency can contribute to the critical analysis of the rhetoric of good and evil, the suspension of constitutional liberties, and the abrogation of international agreements that characterize the “global war on terror.”

#### Policymakers’ attempts to impose order and certainty on the world result in constant war and violence

Burke in 2007

(Anthony, Senior Lecturer in Politics and International Relations at UNSW, Sydney, “Ontologies of War: Violence, Existence and Reason”, Theory & Event, Volume 10, Issue 2, 2007, pMUSE, cheek)

# At the same time, **Kissinger's hubris and hunger for control was beset by a corrosive anxiety: that, in an era of nuclear weapons proliferation and constant military modernisation**, of geopolitical stalemate in Vietnam, and the emergence and militancy of new post-colonial states, **order and mastery were harder to define and impose**. He worried over the way 'military bipolarity' between the superpowers had 'encouraged political multipolarity', which 'does not guarantee stability. **Rigidity is diminished, but so is manageability...equilibrium is difficult to achieve among states widely divergent in values, goals, expectations and previous experience'** (emphasis added). He mourned that 'the greatest need of the contemporary international system is an agreed concept of order'.57 **Here were the driving obsessions of the modern rational statesman based around a hunger for stasis and certainty that would entrench U.S. hegemony**: For the two decades after 1945, our international activities were based on the assumption that technology plus managerial skills gave us the ability to reshape the international system and to bring about domestic transformations in "emerging countries". This direct "operational" concept of international order has proved too simple. **Political multipolarity makes it impossible to impose an American design.** Our deepest challenge will be to evoke the creativity of a pluralistic world, to base order on political multipolarity even though overwhelming military strength will remain with the two superpowers.58 **Kissinger's statement revealed that such cravings for order and certainty continually confront chaos, resistance and uncertainty: clay that won't be worked, flesh that will not yield, enemies that refuse to surrender. This is one of the most powerful lessons of the Indochina wars, which were to continue in a phenomenally destructive fashion for six years after Kissinger wrote these words.** Yet as his sinister, Orwellian exhortation to 'evoke the creativity of a pluralistic world' demonstrated, Kissinger's hubris was undiminished. This is a vicious, historic irony: a desire to control nature, technology, society and human beings that is continually frustrated, but never abandoned or rethought. By 1968 U.S. Secretary of Defense Robert McNamara, the rationalist policymaker par excellence, had already decided that U.S. power and technology could not prevail in Vietnam; **Nixon and Kissinger's refusal to accept this conclusion, to abandon their Cartesian illusions, was to condemn hundreds of thousands more to die in Indochina and the people of Cambodia to two more decades of horror and misery**.59 In 2003 there would be a powerful sense of déja vu as another Republican Administration crowned more than decade of failed and destructive policy on Iraq with a deeply controversial and divisive war to remove Saddam Hussein from power. **In this struggle with the lessons of Vietnam, revolutionary resistance, and rapid geopolitical transformation, we are witness to an enduring political and cultural theme: of a craving for order, control and certainty in the face of continual uncertainty. Closely related to this anxiety was the way that Kissinger's thinking -- and that of McNamara and earlier imperialists** like the British Governor of Egypt Cromer -- **was embedded in instrumental images of technology and the machine: the machine as both a tool of power and an image of social and political order**. In his essay 'The Government of Subject Races' Cromer envisaged effective imperial rule -- over numerous societies and billions of human beings -- as best achieved by a central authority working 'to ensure the harmonious working of the different parts of the machine'.60 **Kissinger analogously invoked the virtues of 'equilibrium', 'manageability' and 'stability' yet, writing some six decades later, was anxious that technological progress no longer brought untroubled control: the Westernising 'spread of technology and its associated rationality**...**does not inevitably produce a similar concept of reality'**.61 # **We sense the rational policymaker's frustrated desire: the world is supposed to work like a machine, ordered by a form of power and governmental reason which deploys machines and whose desires and processes are meant to run along ordered, rational lines like a machine**. Kissinger's desire was little different from that of Cromer who, wrote Edward Said: ...envisions a seat of power in the West and radiating out from it towards the East a great embracing machine, sustaining the central authority yet commanded by it. What the machine's branches feed into it from the East -- human material, material wealth, knowledge, what have you -- is processed by the machine, then converted into more power...the immediate translation of mere Oriental matter into useful substance.62 # **This desire for order in the shadow of chaos and uncertainty** -- **the constant war with an intractable and volatile matter -- has deep roots in modern thought, and was a major impetus to the development of technological reason and its supporting theories of knowledge**. As Kissinger's claims about **the West's Newtonian desire for the 'accurate' gathering and classification of 'data' suggest, modern strategy, foreign policy and Realpolitik have been thrust deep into the apparently stable soil of natural science, in the hope of finding immovable and unchallengeable roots there**. While this process has origins in ancient Judaic and Greek thought, it crystallised in philosophical terms most powerfully during and after the Renaissance. The key figures in this process were Francis Bacon, Galileo, Isaac Newton, and René Descartes, who all combined a hunger for political and ontological certainty, a positivist epistemology and a naïve faith in the goodness of invention. Bacon sought to create certainty and order, and with it a new human power over the world, through a new empirical methodology based on a harmonious combination of experiment, the senses and the understanding. With this method, he argued, we can 'derive hope from a purer alliance of the faculties (the experimental and rational) than has yet been attempted'.63 In a similar move, **Descartes sought to conjure certainty from uncertainty through the application of a new method that moved progressively out from a few basic certainties (the existence of God, the certitude of individual consciousness and a divinely granted faculty of judgement) in a search for pure fixed truths**. Mathematics formed the ideal image of this method, with its strict logical reasoning, its quantifiable results and its uncanny insights into the hidden structure of the cosmos.64 Earlier, Galileo had argued that scientists should privilege 'objective', quantifiable qualities over 'merely perceptible' ones; that 'only by means of an exclusively quantitative analysis could science attain certain knowledge of the world'.65 **Such doctrines of mathematically verifiable truth were to have powerful echoes in the 20th Century, in the ascendancy of systems analysis, game theory, cybernetics and computing in defense policy and strategic decisions, and in the awesome scientific breakthroughs of nuclear physics**, **which unlocked the innermost secrets of matter and energy and applied the most advanced applications of mathematics and computing to create the atomic bomb.** Yet this new scientific power was marked by a terrible irony: **as even Morgenthau understood, the control over matter afforded by the science could never be translated into the control of the weapons themselves, into political utility and rational strategy**.66

#### Risk-assessment of future threats is based in incomplete information---this temporal logic devalues the present to preserve the future

Stockdale, 10

(Liam Stockdale, Ph.D. in International Relations, Department of Political Science, McMaster University. “Securitizing the Future? A Critical Interrogation of the Pre-emptive Turn in the Theory and Practice of Contemporary Security” <https://www.academia.edu/430468/Securitizing_the_Future_A_Critical_Interrogation_of_the_Pre-Emptive_Turn_In_the_Theory_and_Practice_of_Contemporary_Security>) Henge

As mentioned above, an explicitly temporal element has underwritten the development of security practices in the post-9/11 era, and this trend is particularly evident in the activities of what are popularly termed “liberal” or “Western” states.2 Indeed, empirically speaking, the majority of the pre-emptive practices with which I am here concerned take place either within the context of the WOT—such as the indefinite detention of terror suspects without charge (Mutimer 2007)—or vis-à-vis the purported threat of large inflows of migrants—exemplified by the myriad detention centres on the periphery of the EU and by Australia’s so-called “pacific solution” of mandatory pre-emptive detention (Isin & Rygiel 2007, L. Weber 2007). These issues represent top security concerns for states that are conventionally identified as liberal democratic polities, and therefore the pre-emptive practices upon which I focus most often originate from the sovereign decisions undertaken by the governments and security agents of such states. This is important in theoretical terms because the fact that it is precisely states which are “avowedly liberal democratic states, openly committed to the rule of law” (Mutimer 2007) that are behind the types of pre-emptive practices I seek to problematize renders the logic underlying such acts—and perhaps even the concept of the liberal polity itself in the current security moment—quite problematic. This latter point will be central to the second half of the paper—and will be discussed in greater depth below in relation to Derrida’s notion of autoimmunity—and thus a more detailed discussion of pre-emption as it is practiced by contemporary liberal polities is warranted at this juncture. While the idea of pre-emption with regard to discourses of security is perhaps most often associated with the so-called Bush Doctrine in US foreign policymaking—most clearly exemplified, of course, by the 2003 invasion of Iraq (Ehrenberg et al. 2010, C. Weber 2007)—it must also be stressed that the notion of taking explicit action in the present to preempt potential irruptions of “danger” in the future—what might be termed the logic of preemption— is far from limited in its deployment to the realm of interstate security relations alone. Indeed, as criminologist Richard Ericson asserts, the logic of pre-emption can be seen to permeate all aspects of the exercise of sovereign power in the current moment, to the point where the contemporary security environment might be best termed a “state of pre-emption” (Ericson 2008: 58). Under such conditions, “security” is conceived in terms of safeguarding the future from what may occur by undertaking precautionary measures in the present that are conceived in relation to an imagined future. Security is thus pursued by attempting to “police the future by anticipation,” with the ultimate goal being the realization of an imagined “future perfect” where the “risks” against which these present exceptional practices are deployed will no longer be of concern (Bigo 2007: 31). Accordingly, the logic of pre-emption is innately concerned with exerting control over the temporal dimension of human existence. Sovereign power deployed in pursuit of the logic of pre-emption is thus active in both the spatial and temporal realms, as it attempts to manipulate and control the relationship between present and future through “calculations about probable futures in the present [the temporal element], followed by interventions into the present in order to control that potential future [the spatial element]” (Aradau et al. 2008: 149). The crucial point is that a security climate premised upon the logic of pre-emption is concerned primarily with safeguarding the future, while the present is constructed in instrumental terms as a site of intervention through which this ultimate aim might be realized. As such, to use the terminology of the Copenhagen School, under the logic of pre-emption, the future is securitized (Buzan et al. 1998). The result is that the proverbial door is opened for the deployment of exceptional practices “beyond the realm of normal politics” in the present, since the logic of pre-emption holds that it is through proactive/preemptive/ precautionary measures enacted in the present that the security of the future can be ensured. Yet the inherent unknowability of the future ensures that pre-emptive pursuits are necessarily plagued by an information deficit, thus generating “an insatiable quest for knowledge” on the part of sovereign authorities pursuing information related to potential future dangers (Aradau & Van Munster 2007: 91). Regardless of the success of such efforts, however, the idea of pre-emptive security is perpetually imbued with an innate level of uncertainty precisely because the future cannot be known for certain, no matter how detailed and precise and rigorous the collected data and subsequent risk calculations might be (de Goede 2008). This leads the imperatives of pre-emptive security to merge with a politics of risk management premised upon the so-called “precautionary principle,” whereby sovereign decisions relating to appropriate pre-emptive action to be undertaken are made solely on the basis of unsubstantiated suspicion or highly arbitrary (and often highly racialized) calculations regarding the likelihood of a future irruption of threat (Aradau & Van Munster 2007: 102). Accordingly, the pre-emptive practices of sovereign power take on a highly biopolitical character, as governmental intrusions into the everyday lives of individual subjects become an crucial component of the pursuit of security. The securitization of the future thus necessitates the deployment of an extensive array of governmental technologies—from conventional military intervention, to indefinite detention, to pervasive surveillance and biometric monitoring—in pursuit of information that might be relevant to preventing an irruption of danger that may occur in at some indefinite point in the unknown future (Ibid. 105). Aradau and Van Munster (2007: 97), invoking Foucault, aptly refer to these practices collectively as a precautionary “dispositif of risk,” capturing both the variety of techniques employed and the ultimately unified objective of securing an imagined future that underwrites their enaction.

#### A prior understanding of the discursive underpinnings of cyber policy opens up avenues of political choices---we must analyze the supposed truths that establish a reservoir of accepted threat representations

Cavelty, 13

(Dr. Myriam Dunn Cavelty is Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich, Switzerland and was Fellow at the “stiftung neue verantwortung” in Berlin, Germany. She publishes regularly in international journals and has authored and edited several books on information age security issues In addition to her teaching, research and publishing activities, she advises governments, international institutions and companies in the areas of cyber security, cyber warfare, critical infrastructure protection, risk analysis and strategic foresight. As an internationally renowned cyber expert she is a frequent speaker at professional conferences. “From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse” doi: 10.1111/misr.12023) Henge

Matters of cyber-(in)-security—though not always under this name—have been an issue in security politics for at least three decades (Dunn Cavelty 2008).1 As a result, the link between national security and cyberspace has become an uncontested, unshakable “truth” with budgetary and political consequences. However, this link is far more diverse as it is often assumed in the literature. The cybersecurity discourse is about more than one threat form: ranging from computer viruses and other malicious software to cyber-crime activity to the categories of cyber-terror and cyber-war. Each subissue is represented and treated differently in the political process and at different points in time. Consequently, cyber-security policies contain an amalgam of countermeasures, tailored to meet different, and at times conflicting security needs. How these heterogeneous political manifestations are linked to different threat representations—ways to depict what counts as a threat or risk—is the focus of this article. Importantly, and in contrast to most of the other research on the subject, this paper therefore focuses on cyber-security comprehensively,2 rather than looking at discourse in subcategories like cyber-crime, cyber-terrorism, or cyber- war. I argue that only a broad understanding of cyber-security as discursive practice by a multitude of actors inside and outside of government reveals the variety of choices available to political actors at all times and enables us to show what the consequences of such choices are. The paper has four parts. First, the theoretical approach, a cross-over between the linguistic and the sociological (or practice-based) approach of Securitization Theory and discourse theory more broadly, is outlined. Second, the language used to talk about cyberspace is described, as it forms the basis for how security and insecurity in this realm are conceptualized. Third, three key threat representations are identified: the portrayal of malware by using a biological register (virus/worms); the description of disembodied miscreants (hackers); and complex interrelationships between critical infrastructures and the cyber-substructure, and a subsequent emphasis on vulnerability. Fourth, the paper links these threat representations to cyber-security policies and practices (as an indication of their constitutive effects). In conclusion, I reflect on what the choice for specific threat representations and the type of practices they inspire signify for the present and the future of cyber-security. Discursive Practices “Below the Radar” To date, political science literature on cyber-security—and closely related subissues such as cyber-crime, cyber-terrorism, or cyber-war—remains policy-oriented and does not communicate with more general international relations theory, not even neo-realism (Eriksson and Giacomello 2007). There is a notable exception: A limited number of scholars have used frameworks derived from Securitization Theory (Buzan, Wæver, and De Wilde 1998) to establish how different actors in politics have tried to argue the link between the cyber-dimension and national security (cf. Bendrath 2001, 2003; Eriksson 2001; Dunn Cavelty 2008; Hansen and Nissenbaum 2009; Lawson 2011, 2012). First-generation Securitization Theory treats security as a discursive (intersubjective and performative) practice, in which particular actors need to successfully proclaim something a security problem. In other words, links between so-called referent objects and the need to use security political means to secure or protect them need to be forged, argued, and accepted in the political process. Like many other discourse-theoretical approaches, the linguistic variant of Securitization Theory focuses on “politically salient speech acts” by “visible” political figures that can be approved or disproved by the general public (Huysmans 2011:371). Therefore, the emphasis is almost always on official statements by “the heads of states, governments, senior civil servants, high ranked military, heads of international institutions” (Hansen 2006:64). Such a focus reveals the constitutive effects the discursive practices of “capable actors” can have in (world) politics (Weldes and Saco 1996; Campbell 1998). However, approaches focusing on elite expressions neglect how these discursive practices are facilitated or thwarted by preceding and preparatory discursive practices of actors that are not as easily visible.3 This paper starts from the premise that within any given discourse, various actors seek to assert themselves and their pattern of argumentation and to establish a dominant discourse pattern. Arguably, social contests for the legitimate definition of reality do not only take place in the open political arena: Depending on the issue at hand, state and nonstate actors—including special- ized bureaucratic units, consultants, or technical experts—have the capacity to establish “the truth” about certain threats (Huysmans 2006:72; Leonard and Kaunert 2011; also Kingdon 2003), therefore creating a “reservoir” of accepted threat representations on which visible political actors (must) draw. The argument this paper makes is that in order to understand the fundamentals of everyday security political processes, the interplay between political discourse and constitutive effects must also be studied in the realm of “little security nothings” (Huysmans 2011). The emergence of cyberspace is an exceptional opportunity to look at how such a reservoir of threat representations was formed.

## 2AC

### AT---Util

#### Util is slave morality

Anomaly in 2005

(Jonny, Tulane University, “Nietzsche’s Critique of Utilitarianism”, The Journal of Nietzsche Studies”, pMUSE)

In interpreting Nietzsche's attacks on utilitarianism, it is crucial to understand the (often tenuous) connection Nietzsche makes between utilitarianism and Christianity. Because Nietzsche considers utilitarianism a secular offspring of Christian morality, many of his global attacks on utilitarianism resemble his more familiar critique of Christian "slave morality"—the morality of the herd. In particular, Nietzsche contends that utilitarianism inherited Christianity's commitment to the equal worth of each person, and perpetuated its erroneous assumption that a timeless, universal criterion for morality is tenable. Nietzsche's preliminary account of the difference between master morality and slave morality in *Beyond Good and Evil* culminates with the conclusion that "[s]lave morality is essentially a morality of utility" (260). Although Nietzsche develops the notorious distinction between master and slave morality most fully in the *Genealogy*, he articulates the sense in which he considers utilitarianism a form of slave morality in a revealing passage in *Beyond Good and Evil*. Here he speculates that the noble, aristocratic man first identifies himself and those like him (powerful, proud, distinguished men) as good, and then contrasts himself with those he contemptuously regards as "the cowardly, the timid, the petty" and, above all, "those who think only of narrow utility" (*BGE* 260). The noble's power consists not only in his ability to exploit others with his superior acumen or physical strength but also in exercising "power over himself," by refraining from acting on the inclination of pity that characterizes those whom he despises. The slave, conversely, identifies himself negatively; he is part of the group that resents those who unabashedly exercise their power. Nietzsche scorns slave morality because its proponents meekly resign themselves to whatever master morality is not, and yet consider their own moral principles universally binding rather than acknowledging them as narrowly useful for members of their own group. In the Christian tradition, "pity, the kind and helping hand, the warm heart, patience, industriousness, humility, friendliness come into honor—for these are the most *useful* qualities [for the slave]" (*BGE* 260).

### 2AC---FW Top Level

#### Tragedy DA---radical democracy must be open to its own destruction

Hatab in 2002

(Lawrence J, Professor of Philosophy at Old Dominion University, “Prospects for a Democratic Agon: Why We Can Still Be Nietzscheans”, The Nietzsche Journal, pMUSE)

Appel insists that a radical agonistics is a significant threat to democratic ideals and principles. Although he does little to develop how and why this may be so, the charge raises important questions facing postmodern, and particularly Nietzschean, approaches to democratic politics. In my work I have tried to face this question, admit the difficulty, and suggest a "tragic" model of democratic openness, to borrow from Nietzsche's interest in tragedy. [27](http://muse.jhu.edu/journals/journal_of_nietzsche_studies/v024/24.1hatab.html" \l "FOOT27) Many democratic theorists insist that politics must be grounded in secure principles, which themselves are incontestable, so as to rule out anti-democratic voices from having their day and possibly undermining democratic procedures or results. A radically agonistic, open conception of democracy that simply invites any and all parties to compete for favor seems utterly decisionist, with no justification beyond its contingent enactment. But from a historical perspective, despite metaphysical pretenses in some quarters, democratic foundings have in fact emerged out of the "abyss" of conventions and decisional moments. [28](http://muse.jhu.edu/journals/journal_of_nietzsche_studies/v024/24.1hatab.html" \l "FOOT28) And with the prospect of a constitutional convention in our system, it is evident from a performative standpoint that any results are actually possible in a democracy, even anti-democratic outcomes (not likely, but surely possible). The "tragedy" is that democracy could die at its own hands. Foundationalists would call such an outcome contradictory, but a tragic conception would see it as a possibility intrinsic to the openness of democratic practice.

### 2AC---Limits

#### Competition must always be open to the transvaluation of limits---each debate leaves contest radically open to new possibilities---forcing FW debates is a good thing

Acampora, 6

(Christa Davis, professor of philosophy at City University of New York. “CRITICAL AFFINITIES: NIETZSCHE AND AFRICAN-AMERICAN THOUGHT” pg. 183-4)

Given that, he asks, what form of struggle might best advance human possibilities generally? Several features of productive contest emerge, although Nietzsche never offers a full exposition of the relevant question?' Beyond potentially inspiring excellence, which would presumably be relative to some previously existing standard, agonistic contest is supposed to be radically open, at least this seems to be a feature that Nietzsche specifically designates as exceptional about the view he finds in ancient Greece.21 The openness is achieved in two respects: first, the viability of challenge must be preserved; second, the contest must be flexible enough to generate decisions about excellence that are relative not only to past performances but also in accordance with new standards produced through the contest itself. 22 In other words, although rare and exceptional, every contest at least extends the possibility that the prevailing standards of measure themselves could be reformed. The significance of this openness to the community as a whole is evident to Nietzsche in what Diogenes Laertius reports as the original purpose of ostracism: anyone who emerged as an undefeatable opponent had to be banished, as great as such a person might be. This was not because greatness itself was despised; rather, it was out of concern for cultivating the pursuit of excellence as a whole. The latter was to be effected not through reduction to the lowest common denominator but by ever extending the prospect of being able to earn a title to great- ness, to participate in creating the standard for what would count as best. Moreover, those standards of judgment were being constantly formulated and renegotiated in every instance of rendering a decision. Nietzsche cites the most exemplary contestants as those who not only offered an exceptional performance in the contest but also revised the very standards by which they were judged. Nietzsche's admiration of these features of contest makes it clear that he is not simply nostalgic for a heroic ethic of nobility lost, and he is not pining for a return to the good old days of Homer. Moreover, it is worth considering the relations between victors, competitors, and the community that will provide the institutional framework for such agonistic enterprises to occur.

### 2AC---Extinction Impacts

#### Human extinction is inevitable---gwarm tipping points

Curry, 13

(Nathan Curry, Vice. “SOME CREDIBLE SCIENTISTS BELIEVE HUMANITY IS IRREPARABLY CLOSE TO DESTRUCTION” <http://www.vice.com/en_ca/read/near-term-extinctionists-believe-the-world-is-going-to-end-very-soon>) Henge

If you were to zoom out and take a comparative look back at our planet during the 1950s from some sort of cosmic time-travelling orbiter cube, you would probably first notice that millions of pieces of space trash had disappeared from orbit. The moon would appear six and a half feet closer to Earth, and the continents of Europe and North America would be four feet closer together. Zooming in, you would be able to spot some of the industrial clambering of the Golden Age of Capitalism in the West and some of the stilted attempts at the Great Leap Forward in the East. Lasers, bar codes, contraceptives, hydrogen bombs, microchips, credit cards, synthesizers, superglue, Barbie dolls, pharmaceuticals, factory farming, and distortion pedals would just be coming into existence. There would be two thirds fewer humans on the planet than there are now. Over a million different species of plants and animals would exist that have since gone extinct. There would be 90 percent more fish, a billion less tons of plastic, and 40 percent more phytoplankton (producers of half the planet’s oxygen) in the oceans. There would be twice as many trees covering the land and about three times more drinking water available from ancient aquifers. There would be about 80 percent more ice covering the northern pole during the summer season and 30 percent less carbon dioxide and methane in the atmosphere. The list goes on... Most educated and semi-concerned people know that these sorts of sordid details make up the backdrop of our retina-screened, ethylene-ripened story of progress, but what happens when you start stringing them all together? If Doomsday Preppers, the highest rated show on the National Geographic Channel is any indication, the general public seems to be getting ready for some sort of societal collapse. There have always been doomsday prophets and cults around and everyone has their own personal view of how the apocalypse will probably go down (ascension of pure souls, zombie crows), but in the midst of all of the Mayan Calendar/Timewave Zero/Rapture babble, there are some clarion calls coming from a crowd that’s less into bugout bags and eschatology: well-respected scientists and journalists who have come to some scarily-sane sounding conclusions about the threat of human-induced climate change on the survival of the human species. Recent data seems to suggest that we may have already tripped several irrevocable, non-linear, positive feedback loops (melting of permafrost, methane hydrates, and arctic sea ice) that make an average global temperature increase of only 2°C by 2100 seem like a fairy tale. Instead, we’re talking 4°C, 6°C, 10°C, 16°C (????????) here. The link between rapid climate change and human extinction is basically this: the planet becomes uninhabitable by humans if the average temperature goes up by 4-6°C. It doesn’t sound like a lot because we’re used to the temperature changing 15°C overnight, but the thing that is not mentioned enough is that even a 2-3°C average increase would give us temperatures that regularly surpass 40°C (104°F) in North America and Europe, and soar even higher near the equator. Human bodies start to break down after six hours at a wet-bulb (100% humidity) temperature of 35°C (95°F). This makes the 2003 heat wave in Europe that killed over 70,000 people seem like not a very big deal. Factoring in the increase we’re already seeing in heat waves, droughts, wildfires, massive storms, food and water shortages, deforestation, ocean acidification, and sea level rise some are seeing the writing on the wall: We’re all gonna die!

### AT: B/I/W ’13—General

#### Correlation with stability doesn’t imply causality—Brooks et al oversell benefits and ignore drawbacks

Walt 1-2 Stephen M. Walt, professor of international affairs at Harvard’s Kennedy School of Government, “More or less: The debate on U.S. grand strategy,” 1/2/2013, http://walt.foreignpolicy.com/posts/2013/01/02/more\_or\_less\_the\_debate\_on\_us\_grand\_strategy

Third, B, I, & W give "deep engagement" full credit for nearly all the good things that have occurred internationally since 1945 (great power peace, globalization, non-proliferation, expansion of trade, etc.), even though the direct connection between the strategy and these developments remains contested. More importantly, they absolve the strategy from most if not all of the negative developments that also took place during this period. They recognize the events like the Indochina War and the 2003 war in Iraq were costly blunders, but they regard them as deviations from "deep engagement" rather than as a likely consequence of a strategy that sees the entire world as of critical importance and the remaking of other societies along liberal lines as highly desirable if not strategically essential.

### UQ—Decline Now

#### Decline now—rising challengers and erosion in political, military and economic cred

Layne ’12 Christopher Layne, Robert M. Gates Chair in Intelligence and National Security at the George Bush School of Government and Public Service at Texas A&M University, noted neorealist, “This Time It’s Real: The End of Unipolarity and the *Pax Americana*,” International Studies Quarterly (2012) 56, 203-213

Some twenty years after the Cold War’s end, it now is evident that both the 1980s declinists and the unipolar pessimists were right after all. The Unipolar Era has ended and the Unipolar Exit has begun. The Great Recession has underscored the reality of US decline, and only ‘‘denialists’’ can now bury their heads in the sand and maintain otherwise. To be sure, the Great Recession itself is not the cause either of American decline or the shift in global power, both of which are the culmination of decades-long processes driven by the big, impersonal forces of history. However, it is fair to say the Great Recession has both accelerated the causal forces driving these trends and magnified their impact. There are two drivers of American decline, one external and one domestic. The external driver of US decline is the emergence of new great powers in world politics and the unprecedented shift in the center of global economic power from the EuroAtlantic area to Asia. In this respect, the relative decline of the United States and the end of unipolarity are linked inextricably: the rise of new great powers—especially China—is in itself the most tangible evidence of the erosion of the United States’ power. China’s rise signals unipolarity’s end. Domestically, the driver of change is the relative—and in some ways absolute—decline in America’s economic power, the looming fiscal crisis confronting the United States, and increasing doubts about the dollar’s long-term hold on reserve currency status. Unipolarity’s demise marks the end of era of the post-World War II Pax Americana. When World War II ended, the United States, by virtue of its overwhelming military and economic supremacy, was incontestably the most powerful actor in the international system. Indeed, 1945 was the United States’ first unipolar moment. The United States used its commanding, hegemonic position to construct the postwar international order—the Pax Americana— which endured for more than six decades. During the Cold War, the Pax Americana reflected the fact that outside the Soviet sphere, the United States was the preponderant power in the three regions of the world it cared most about: Western Europe, East Asia, and the Persian Gulf. The Pax Americana rested on the foundational pillars of US military dominance and economic leadership and was buttressed by two supporting pillars: America’s ideological appeal (‘‘soft power’’) and the framework of international institutions that the United States built after 1945. Following the Cold War’s end, the United States used its second unipolar moment to consolidate the Pax Americana by expanding both its geopolitical and ideological ambitions. In the Great Recession’s aftermath, however, the economic foundation of the Pax Americana has crumbled, and its ideational and institutional pillars have been weakened. Although the United States remains preeminent militarily, the rise of new great powers like China, coupled with US fiscal and economic constraints, means that over the next decade or two the United States’ military dominance will be challenged. The decline of American power means the end of US dominance in world politics and a transition to a new constellation of world power. Without the ‘‘hard’’ power (military and economic) upon which it was built, the Pax Americana is doomed to wither in the early twenty-first century. Indeed, because of China’s great-power emergence, and the United States’ own domestic economic weaknesses, it already is withering.

### 1NC—Unsustainable

#### Heg collapse inevitable—structural economic weakness

Layne ’12 Christopher Layne, Robert M. Gates Chair in Intelligence and National Security at the George Bush School of Government and Public Service at Texas A&M University, noted neorealist, “This Time It’s Real: The End of Unipolarity and the *Pax Americana*,” International Studies Quarterly (2012) 56, 203-213

Contrary to the way their argument was portrayed by many of their critics, the 1980s declinists did not claim either that the United States already had declined steeply, or that it soon would undergo a rapid, catastrophic decline. Rather, they pointed to domestic and economic drivers that were in play and which, over time, would cause American economic power to decline relatively and produce a shift in global distribution of power. The declinists contended that the United States was afflicted by a slow—’’termite’’—decline caused by fundamental structural weaknesses in the American economy.7 Kennedy himself was explicitly looking ahead to the effects this termite decline would have on United States’ world role in the early twenty-first century. As he wrote, ‘‘The task facing American statesman over the next decades. .. is to recognize that broad trends are under way, and that there is a need to ‘manage’ affairs so that the relative erosion of the United States’ position takes place slowly and smoothly, and is not accelerated by policies which bring merely short-term advantage but longer-term disadvantage’’ (Kennedy 1987:534; my emphasis). When one goes back and re-reads what the 1980s declinists pinpointed as the drivers of American decline, their analyses look farsighted because the same drivers of economic decline are at the center of debate today: too much consumption and not enough savings; persistent trade and current account deficits; chronic federal budget deficits and a mounting national debt; and de-industrialization. Over time, 1980s declinists said, the United States’ goals of geopolitical dominance and economic prosperity would collide. Today, their warnings seem eerily prescient. Robert Gilpin’s 1987 description of America’s economic and grand strategic plight could just as easily describe the United States after the Great Recession: With a decreased rate of economic growth and a low rate of national savings, the United States was living and defending commitments far beyond its means. In order to bring its commitments and power back into balance once again, the United States would one day have to cut back further on its overseas commitments, reduce the American standard of living, or decrease domestic productive investment even more than it already had. In the meantime, American hegemony was threatened by a potentially devastating fiscal crisis. (Gilpin 1987:347–348) In the Great Recession’s wake—doubly so since it is far from clear that either the United States or global economies are out of the woods—the United States now is facing the dilemmas that Gilpin and the other declinists warned about.

### 1NC—Heg Bad—Cooperation

#### Stable rise of the rest is key to control prolif, terrorism, failed states, and the economy

Larson ‘10 (Debra Welch, Professor of Political Science at the University of California, Los Angeles, and Alexei Shevchenko, Assistant Professor of Political Science at California State University, Fullerton, Spring, [www.mitpressjournals.org/doi/pdf/10.1162/isec.2010.34.4.63])

Since the end of the Cold War, scholars and foreign policy analysts have debated the type of world order that the United States should strive to create—a hegemonic system, a multilateral institutional system, or a great power concert. 1 Initially, a major issue was whether attempts to maintain U.S. primacy would stimulate counterbalancing from other states. 2 But since the 2003 Iraq War, a new consideration has emerged—how to persuade other states to cooperate with U.S. global governance. 3 States that do not oppose efforts by the United States to maintain stability may nonetheless decline to follow its leadership. This is a matter for concern because although the United States can act alone, it cannot succeed on such issues as controlling terrorism, curbing proliferation of weapons of mass destruction (WMD), rebuilding failed states, or maintaining economic stability without help from other states. Among the states whose support is critical are China and Russia. China, which in modern times has never been accorded great power status, has experienced impressive economic growth and is rapidly rising in the international system. China’s ascendance creates expectations of an uncertain power transition in the Asia-Pacific region and potentially in world politics, one that could be accompanied by dangerous competition. Then there is Russia, a former superpower and (after a decade of post-Soviet retrenchment complicated by gross internal mismanagement) most recently a resurgent power because of a rise in energy prices, a power that has not yet found a place in world politics. Obtaining cooperation from China and Russia is more complex and difficult because they are outsiders from the liberal Western community, with differing values and interests. 4 In contrast, as a long-standing democracy, rising power India is more susceptible to appeals to common values, especially since the 2006 nuclear agreement with the United States recognized India’s status as a nuclear power. 5 With China and Russia, the problem is how to obtain their cooperation with U.S. global governance if they cannot be integrated into the West. The United States needs Chinese and Russian assistance to curb proliferation of WMD, control terrorism, maintain stable energy supplies, and stabilize Eurasia. China and Russia have permanent seats on the United Nations (UN) Security Council, allowing them to veto resolutions authorizing intervention or sanctions against would-be proliferators or aggressors. China and Russia also have political ties with Iran and North Korea that could make them useful intermediaries. Because of its economic aid and geographic proximity, China is an essential interlocutor with North Korea; Russia is a major arms supplier and economic partner with Iran. Russia has thousands of nuclear weapons and tons of nuclear materials, both coveted by rogue states and terrorist groups. As the second-largest oil exporter and the holder of the world’s largest gas reserves, Russia can affect global energy supplies and prices. Russia could provide help as a transit route for U.S. military supplies and source of intelligence for the U.S. effort to stabilize Afghanistan. As the dominant power in Central Asia, Russia can assist in maintaining stability in this energy-rich region, an area that is increasingly important to China as well. The United States needs to work with China to stabilize security relationships in the Asia-Paciªc region, head off regional rivalries, and prevent dangerous conºict resulting from a North Korean implosion. Scholars have debated whether future Chinese and Russian foreign policies will contribute to global stability. 6 Both states have been reluctant to agree to tough sanctions on North Korea and Iran to stop their nuclear programs. 7 As China’s consumption of energy has grown, Beijing has been actively competing for control of energy resources around the world, sometimes in rogue states such as Burma, Iran, and Sudan. 8 China has used the growing wealth of its economy to modernize its military, increasing its ability to coerce Taiwan or seize disputed territory in the East and South China Seas. 9 Russia has been trying to exert inºuence over the post-Soviet space by such means as cutting off the supply of oil and gas, 10 and most dramatically, its August 2008 incursion into Georgia followed by recognition of the breakaway republics Abkhazia and South Ossetia. 11 Both China and Russia have sold arms to objectionable regimes such as Burma, Iran, Syria, and Venezuela. 12 Securing Chinese and Russian cooperation requires understanding the objectives and logic of their grand strategies and devising effective policies to achieve that goal. In what follows, we demonstrate that despite apparent shifts and turns, Chinese and Russian foreign policies since the end of the Cold War have been motivated by a consistent objective—to restore both countries’ great power status. We argue that China and Russia will be more likely to participate in global governance if the United States can find ways to recognize their distinctive status and identities. States’ concerns about their relative status have been largely overlooked by the dominant theoretical approaches of neorealism and liberalism. 13 Neorealism focuses on material components of power, whereas liberalism is oriented around norms, institutions, and economic interdependence. These approaches have limited utility for persuading China and Russia to cooperate because neither country needs economic or security assistance from the West, and they do not subscribe to Western liberal democratic norms. For insights into the role of status in international politics, we draw on social identity theory (SIT), which explores how social groups strive to achieve a positively distinctive identity. 14 When a group’s identity is no longer favorable, it may pursue one of several strategies: social mobility, social competition, or social creativity. Social mobility emulates the values and practices of the higher-status group with the goal of gaining admission into elite clubs. Social competition tries to equal or surpass the dominant group in the area on which its claims to superior status rest. Finally, social creativity reframes a negative attribute as positive or stresses achievement in a different domain. Applied to international relations, SIT suggests that states may improve their status by joining elite clubs, trying to best the dominant states, or achieving preeminence outside the arena of geopolitical competition. 15 We apply a theoretical framework based on SIT to case studies of changes in Chinese and Russian grand strategy since the end of the Cold War as a plausibility probe. 16 Our study indicates that China and Russia initially sought great power status through partial acceptance of Western capitalist norms but were denied integration into elite Western clubs. Both states turned to more competitive policies but did not enhance their relative standing. Rather than adjust to the U.S.-led liberal democratic system, China and Russia sought to develop new, more positive images by contributing to global governance while maintaining distinctive identities. China has been remarkably successful in changing other states’ perceptions of its identity, whereas Russia’s cooperation was largely taken for granted. Russia’s foreign policy is currently in a transitional phase with some elements of social competition. Our case studies suggest that the desire for greater status may motivate rising powers to take on more responsibility for maintaining world order. For this outcome to occur, the dominant power, the United States, must offer recognition of the rising state’s more positive identity and status. Overall U.S. predominance allows the United States to recognize other countries’ achievements and contributions in the area of global governance without detracting from its own status. Use of status incentives should receive greater consideration as a tool of global governance. We begin by discussing the basic propositions of SIT, showing why groups are motivated to achieve positive distinctiveness. We then elaborate and conceptualize the SIT typology of identity management strategies, providing applications to international relations. This theoretical framework is then used to explain major shifts in Chinese and Russian grand strategy since the end of the Cold War, and especially the adoption of more cooperative policies. The conclusion identiªes contributions of SIT to understanding otherwise puzzling Chinese and Russian behavior.

### 1NC—Epistemology K

#### Heg impacts are exaggerated to mobilize domestic support

Layne ’97 Christopher Layne, Visiting Associate Professor at the Naval Postgraduate School, “From Preponderance to Offshore Balancing,” International Security, Summer 1997

The security/interdependence nexus results in the exaggeration of threats to American strategic interests because it requires the United States to defend its core interests by intervening in the peripheries. There are three reasons for this. First, as Johnson points out, order-maintenance strategies are biased inherently toward threat exaggeration. Threats to order generate an anxiety “that has at its center the fear of the unknown. It is not just security, but the pattern of order upon which the sense of security depends that is threatened.”4’ Second, because the strategy of preponderance requires U.S. intervention in places that concededly have no intrinsic strategic value, U.S. policymakers are compelled to overstate the dangers to American interests to mobilize domestic support for their policies.42 Third, the tendency to exaggerate threats is tightly linked to the strategy of preponderance’s concern with maintaining U.S. credibility. The diplomatic historian Robert J. McMahon has observed that since 1945 U.S. policymakers consistently have asserted that American credibility is “among the most critical of all foreign policy objectives.” As Khalilzad makes clear, they still are obsessed with the need to preserve America’s reputation for honoring its security commitments: “The credibility of U.S. alliances can be undermined if key allies, such as Germany and Japan, believe that the current. arrangements do not deal adequately with threats to their security. It could also be undermined if, over an extended period, the United States is perceived as lacking the will or capability to lead in protecting their interests.” Credibility is believed to be crucial if the extended deterrence guarantees on which the strategy of preponderance rests are to remain robust. Preponderance’s concern with credibility leads to the belief that U.S. commitments are interdependent. As Thomas C. Schelling has put it: “Few parts of the world are intrinsically worth the risk of serious war by themselves. but defending them or running risks to protect them may preserve one’s commitments to action in other parts of the world at later times.”45 If others perceive that the United States has acted irresolutely in a specific crisis, they will conclude that it will not honor its commitments in future crises. Hence, as happened repeatedly in the Cold War, the United States has taken military action in peripheral areas to demonstrate—both to allies and potential adversaries—that it will uphold its security obligations in core areas.

## 1AR

#### Ascetic ressentiment is the result of any attempt to imagine a better world---we should embrace it as it is

Turanli, 03

(The Journal of Nietzsche Studies 26 (2003) 55-63, Nietzsche and the Later Wittgenstein: An Offense to the Quest for Another World, Aydan Turanli, Professor, Department of Humanities and Social Sciences, Istanbul Technical University)

The craving for absolutely general specifications results in doing metaphysics. Unlike Wittgenstein, Nietzsche provides an account of how this craving arises. The creation of the two worlds such as apparent and real world, conditioned and unconditioned world, being and becoming is the creation of the ressentiment of metaphysicians. Nietzsche says, "to imagine another, more valuable world is an expression of hatred for a world that makes one suffer: the ressentiment of metaphysicians against actuality is here creative" (WP III 579). Escaping from this world because there is grief in it results in asceticism. Paying respect to the ascetic ideal is longing for the world that is pure and denaturalized. Craving for frictionless surfaces, for a transcendental, pure, true, ideal, perfect world, is the result of the ressentiment of metaphysicans who suffer in this world. Metaphysicians do not affirm this world as it is, and this paves the way for many explanatory theories in philosophy. In criticizing a philosopher who pays homage to the ascetic ideal, Nietzsche says, "he wants to escape from torture" (GM III 6). The traditional philosopher or the ascetic priest continues to repeat, "'My kingdom is not of this world'" (GM III 10). This is a longing for another world in which one does not suffer. It is to escape from this world; to create another illusory, fictitious, false world. This longing for "the truth" of a world in which one does not suffer is the desire for a world of constancy. It is supposed that contradiction, change, and deception are the causes of suffering; in other words, the senses deceive; it is from the senses that all misfortunes come; reason corrects the errors; therefore reason is the road to the constant. In sum, this world is an error; the world as it ought to be exists. This will to truth, this quest for another world, this desire for the world as it ought to be, is the result of unproductive thinking. It is unproductive because it is the result of avoiding the creation of the world as it ought to be. According to Nietzsche, the will to truth is "the impotence of the will to create" (WP III 585). Metaphysicians end up with the creation of the "true" world in contrast to the actual, changeable, deceptive, self-contradictory world. They try to discover the true, transcendental world that is already there rather than creating a world for themselves. For Nietzsche, on the other hand, the transcendental world is the "denaturalized world" (WP III 586). The way out of the circle created by the ressentiment of metaphysicians is the will to life rather than the will to truth. The will to truth can be overcome only through a Dionysian relationship to existence. This is the way to a new philosophy, which in Wittgenstein's terms aims "to show the fly the way out of the fly-bottle"

#### And acknowledgement of the meaninglessness inherent to life is key to creating value

Diamantides in 2003

(Dr. Marinos, Senior Lecturer in Law, University of London, SYMPOSIUM: NIETZCHE AND LEGAL THEORY (PART II): THE COMPANY OF PRIESTS: MEANINGLESSNESS, SUFFERING AND COMPASSION IN THE THOUGHTS OF NIETZSCHE AND LEVINAS, Cardozo Law Review, March, 2003, l/n)

In relation to the classical philosophical problem posed by suffering there is, as the two quotes above indicate, an intriguing common emphasis on meaninglessness in the works of Nietzsche and Levinas, which renders fertile the reading together of their two distinct philosophies. The difference is that for Levinas, the acknowledgement of the meaninglessness of suffering without resentment is only the "least one can say." Indeed, Nietzsche exposed man's denial of absurd suffering "only" in order to support his case against the sentimentalism of Christian ethics and deontological and utilitarian moralities, which either attribute meaning to suffering or seek to rid life of it, ultimately denying life itself - for to live is also to suffer. Levinas, on the other hand, argued the inevitability of events of senseless suffering breaching from within the hermeneutically ordered world of meaning. Moreover, he viewed this as proof of the inevitability of the idea of infinity in a non-metaphysical sense, for it is "included" into the finite world of being as what cannot be matched by experience or representation, leaving a surplus of awe, astonishment, obsession. Immanence, therefore, is all there is, but to that we add that it cannot cease undergoing the idea of infinity, like an ill man who undergoes his condition. In Levinas' ethical discourse, infinity gets expressed in the "face of the other" and is transformed into obsession with providing succors for meaningless suffering. Suffering, left to its own devices, ridicules experience by always being "too much." In turn, it takes another being that comes to the rescue, thinking itself "infinitely responsible" for all the suffering it encounters, for suffering to be given an appropriate response. With this quasi-transcendental possibility in mind, this paper introduces and critically analyzes Nietzsche's notion of "affirmative compassion," as distinct from moral pity and, gradually, suggests the need for its reformulation as both an instance of will to power and as submission to the ethical imperative to care for the other. Given the un-saintly reputation of Nietzsche, however, the paper cannot but begin by paying tribute to his famous critique of pity, that "morbid emotion" that accompanies the denial of the senselessness of suffering and ultimately compels the nihilistic rejection of life itself. This is done in the first section in which I basically report on my law students' take on Nietzsche in the context of a course on medical law and moral reasoning. In sum, I report that Nietzsche's ideas help one critique the extensions of  [\*1277]  traditional legal doctrines of responsibility for man-made harm - sustained by the beliefs in the causal understanding of the world, in moral autonomy and agency - in relation to litigation that raises questions over the meaning of, and standard of care for, suffering that no one has caused. These doctrinal extensions are, arguably, instances of a hypertrophy of legal consciousness, indicating lack of understanding of the chaotic nature of the world of human affects in the face of absurd suffering and denial of the passion, obsession and delirium that correlate to the dis-equilibrium, meaninglessness and anarchy of suffering. In this connection, I offer a number of examples, often involving judgments that concern kinds of beings that blatantly manifest this senselessness, ranging from insensate beings in coma to the unborn. In the second section, I examine Nietzsche's views on how meaningless suffering affects the man of power. Because of Nietzsche's conviction that cruelty and indifference are no longer options for contemporary man, I focus on Nietzsche's formulation of a "noble compassion" that would be "affirmative" or "life-enhancing" - compassion within a meaningless universe. Such compassion is part of the becoming of beings with a "surplus of power," as opposed to morally submissive or hedonistic beings. Crucially, this is compassion that does not relinquish self-love in the process, and does not lead to the self becoming physically or emotionally "contaminated" by the suffering it witnesses.