Securitization and the Global Politics of Cybersecurity

Dr Mark Lacy, Politics, Philosophy and Religion, Lancaster University

Dr Daniel Prince, School of Computing and Communication, Lancaster University

Introduction

In ‘Digital Disaster, Cyber Security, and the Copenhagen School,’ published in 2009, Lene Hansen and Helen Nissenbaum suggest ways in which securitization theory can help us understand the politics of cybersecurity and cyberwar, a complex terrain that brings together a variety of technical and policy challenges that range from individual cybersecurity problems (cybercrime) through to issues of national and economic cybersecurity (anxieties about attacks on ‘critical infrastructure’) (Hansen and Nissenbaum, 2009). Some of the threats point to futuristic ‘black swan’ disasters that result from our high-speed networked society; some of the challenges are traditional problems – abuse and harassment, grooming and recruitment, identity theft and fraud – carried out with new technologies. The cyber-terrain is one where there is an anxiety that an individual can become a national security problem in new and dangerous ways – and where cyber techniques and technologies of national security can play out at the level of the individual in new and unprecedented ways, with innovations in the surveillance and monitoring of everyday life: the security state becomes - to use the fashionable management term - increasingly *granular*. This essay returns to Hansen and Nissenbaum’s article, an article that introduced new complexities, questions and nuances to the study of cybersecurity in security studies and international relations, to think about the changing terrain of cybersecurity in the second decade of the Twenty First Century– and the importance (and problems) of thinking about the ‘non-West’ in research on (cyber)securitization.

Hansen and Nissenbaum are interested in how the collective ‘referent objects’ of ‘the state,’ ‘society,’ ‘the nation’ and ‘the economy’ are presented as being threatened through three types of securitization that ‘tie referent objects and securitizing actors together’(Ibid, p.1163): hypersecuritization, everyday security practices and technifications. On this view, hypersecuritzation refers to the expansion of a security problem into a realm where there is the danger that threats can be exaggerated, resulting in excessive countermeasures: these hypersecuritizations, according to Hansen and Nissenbaum, always ‘mobilize the spectre of the future’ while also using ‘the past as a legitmating reference’(Ibid, p.1164). In the public threat horizon of future threats and dangers, proponents of cyber fears often use historical analogies of ‘electronic pearl habors’ or ‘cyber 9/11s’ in speculations on new types of threats: for the securitization theorists, the ‘re-animation’ of past events works to give a ‘form’ or credibility to future threats that have yet to occur – or are yet to be imagined.

What was significant about Hansen and Nissenbaum's essay was the way it attempted to add new approaches and questions to a topic that tended to occupy a space in an often highly technical discourse of security, technology and strategy, a discourse that extended in to all aspects of life in a digitizing society. Indeed, 'everyday security practices' in their work refers to the ways that individuals and organizations are integrated into the practices of securitization as 'both a responsible partner in fighting insecurity' and also as a potential threat, allowing for responses that can permeate all aspects of everyday life (Ibid, p.1165). This was a discourse of security that due to the technical complexity was presented as occupying the 'cutting edges' of security, a zone that few outside of computer science would be able to engage with. In this sense, 'technification' refers to the manner in which cybersecurity becomes a terrain that depends on the 'expert authority' of the computer scientist and policy expert for its legitimacy, a domain where 'the experts' are the securitizing actors in a manner that risks to detach the issues from critical scrutiny and dialogue. Using the case study of Estonia in April-May in 2007 the authors illustrate how securitization theory can bring conceptual clarity and complexity to a terrain that can either be reduced to simplifications using the past as a means of understanding – or taking the issues into a zone where it is beyond our means of critical understanding and comprehension, where we feel overpowered by our inability to engage critically with the issues, issues that can leave us with the feeling we are in the realm of *geopolitical science fictions*, a world that feels increasingly like the 'cyberpunk' novels of William Gibson or films such as *Ghost in the Shell*.

Hansen and Nissenbaum reach a conclusion that resonates with the broader objectives of securitization theory and 'critical security studies': to develop strategies to counter and interrogate the 'exceptional' status of security issues – where an issue might be presented as 'exceptional' due to the threat to the national interest and/or exceptional due to the technical knowledge needed to evaluate the threat:

> Cyber securitizations are particularly powerful precisely because they involve a double move out of the political realm: from the politicized to the securitized, from the political to the technified, and it takes an inter-disciplinary effort to assess the implications of the move, and possibly to counter it…cyber security stands at the intersection of multiple disciplines and it is important that both analysis and academic communication is brought to bear on it. The technical underpinnings of cyber security require, for instance, that IR scholars acquire some familiarity with the main technical methods and dilemmas, and vice versa that computer scientists become more cognizant of the politicized field in which they design and how their decisions might impact the (discursively constituted) trade-offs between security, access, trust, and privacy (Ibid, p. 1172).

The implication of this argument is an important one: we should develop the tools that enable us to challenge the ethico-political dangers of hypersecuritization in this rapidly changing (cyber) space; to be able to see into this zone of expert knowledge and authority, the spaces where decisions are made on the policies and technologies that will shape all areas of war and security (see Balzacq, 2011). But this essay asks: what should IR scholars be doing in addition to the challenge and task – to become more inter-disciplinary in order to be able to engage with the potential technification and hypersecuritizations of cybersecurity policy and discourse – that was set out in Hansen and Nissenbaum's article?

What we want to do in this essay is suggest that in the time since the essay was published there may be problems and trends that have emerged that require some additional approaches to this issue of hypersecuritization and technification. Simply put, we need to think again about the problems of cybersecurity in the 'political realm' and we need to develop research on cybersecurity and 'political realms' in different places around the planet; to go beyond the often hypersecuritizing images of digital danger and 'otherness' emerging from the 'non-West' to explore the complexity of cybersecurity both from the perspective of new 'everyday security strategies' that individuals may confront but also in terms of the potential for 'digital disasters' that might emerge from specific technological, legal, political and security contexts.

Following on from Hansen and Nissenbaum, our position in the paper begins from the view that inter-disciplinary attempts to engage critically with hypersecuritization is the primary task of work in this space: to be able to counter hypersecuritizations where threats are 'hyped up' - or unspecified future cyber dangers are invoked - is the first move for scholars who want to think critically about the 'threat horizons' that we are presented with on the (not so) clear and present/future dangers. In the time since the essay has been published (2009) much of the debate has centred around the hyper securitization of the concern with all things digital and the implications for the future of security and war (most notably in Thomas Rid's book *Cyberwar Will Not Take Place*). At the same time, there have also been events that have pointed to the possibility of the types of future problems that we could confront – from events that fit with the type of warnings on digital disaster that many have been making since the issue emerged (the hacking of Ukrainian power grids, the Central Bank of Bangladesh bank heist) to the emergence of events that were not considered in previous speculations on digital disaster (Zetter, 2016a; Zetter, 2016b) : attempts to shape the political direction of other states through a combination of disruptive 'gray zone' tactics that may involve hacking and new uses of social media (the debate over 'fake news' and social media, the U.S. Presidential election in 2016). The problem now is not simply hypersecuritization but the problem of what Ulrich Beck describes as 'organized irresponsibility' where the 'state administration, politics, industrial management and research negotiate the criteria of what is 'rational and safe.'' Discussing environmental risks, Beck asks 'do we live in the context of 'organized irresponsibility'?'(Beck, 1999, p.6). We would suggest the same question needs to be asked in the context of the securitization of digital risks and insecurities.

What we suggest in the article is this: once we have established that the first move in this area is think critically about cyber securitizations and the potential problems of the move from the political to the technified, we can consider the concerns of those who we describe as the 'cyber catastrophists' – those who continue to be concerned about the digital disasters that could impact on all aspects of life. We suggest that in this realm of cybersecurity we see three positions that shape the ideas that are contributing to vibrant debate and discussion of the future of cyberwar and cybersecurity: the cyber catastrophist, the digital realist and the techno optimist. The essay rests on the position that each perspective presents us with questions about cybersecuritizations that we need to constantly remain open to – given the fast-moving and disruptive pace of geopolitical and technological change. We suggest that the point in Hansen and Nissenbaum's essay about the need to counter hypersecuritizations needs to be supplemented by more exploratory questions about whether we confront the issue of organized irresponsibility in this space. The problem of technification is not simply on how it might add legitimacy to hypersecuritization, in what it enables us to visualize in the imagination of digital disaster – it is what it fails to see or ignores, the construction and legitimation of what is rational and safe. In other words, we need to examine the politics – and the different positions that may shape policy – in the spaces where important 'expert' decisions are made: to examine, for example, how risk and unintended consequence are being integrated into planning. But the questions opened up by the 'deconstruction' of cybersecurity and cyberwar by Hansen and Nissenbaum also point to inquiry on the changing nature of 'everyday security practices' and here we suggest that is clearer now is the need for IR scholars to examine the specific contexts, controversies and challenges in diverse spaces beyond the often simplistic geographies of cyber-threat that often serve to fuel the hypersecuritized visions of geopolitical imaginaries.

One of the geopolitical anxieities that circulates in many of the key positions we discuss is a concern with the cyber insecurities that we confront from the non-West or that may result from poor cyber governance in the non-West. While this use of the term 'non-West' can be problematic and limiting it does remind us to think beyond the simplistic geography of 'cyber' danger that is often central to the debates about cybersecurity, the geopolitical imaginary filled with devious Bond- villains from former Communist-countries, cunning- 'Oriental' cyber criminals from a cyberpunk movie, totalitarian states experimenting with new technologies of *Minority Report*-like control and 'feral' digital environments in states outside the 'tame zones' of global politics. Securitization perspectives – along with work influenced by poststructuralist writers – are often a call to see beyond the simplistic representations of global politics that continue to imagine the future through the same geographies of otherness and difference that shaped the past (Hansen, 2006). This article suggests that – in the spirit of Hansen and Nissenbaum's essay – we need to keep searching for the questions that need to be asked about a terrain that more than ever needs to be examined in its fast moving complexity and messiness: to examine the difference, complexity and messiness of new trends, practices and behaviours in environments that are often ignored or reduced to the 'same' in a supposedly homogenizing and universalising global technological culture.

The Cyber Catastrophist, the Digital Realist, and the Techno Optimist

The Cyber Catastrophist

The cyber catastrophist suggests that digital disaster is on the threat horizon – and it is often *underplayed* in the discourses of geopolitical danger. Few catastrophists, however, would see digital disasters resulting in social, economic and infrastructural collapse similar to the violence made possible by weapons of mass destruction. But there are exceptions. In *Global Trends 2030: Alternative Worlds* - the fifth instalment of the National Intelligence Councils reports on the future of global security and economy - the report includes a list of 'Potential Black Swans That Would Cause the Greatest Disruptive Impact':

> Nuclear powers such as Russia and Pakistan and potential aspirants such as Iran and North Korea see nuclear weapons as compensation for other political and security weaknesses, heightening the risk of their use. The chance of nonstate actors conducting a cyber attack – or using WMD – also is increasing.(National Intelligence Council, 2012, p.xi)

What is interesting here– in a measured report not prone to doom-mongering or panic – is the partnering of cyber with the more traditional threat of nuclear attack and weapons of mass destruction. Although the exact nature of the consequences are left vague and unspecified, what is interesting for us is this move to frame cybersecurity or cyber-weapons on the same level as weapons of mass destruction, a potentially hyper-securitizing move that includes non-state actors as potential contributors to digital disaster.

This anxiety about the potential capabilities of 'non-traditional' actors with 'non-traditional' weapons circulates in many speculations on future insecurity. The United States' Third Offset Strategy sets out to explore the cutting edge of technology, to try to 'stay ahead' of the enemy in a terrain where non-state actors might become a threat in a traditional sense and where state actors might become a threat in a non-traditional sense, operating in the 'gray zone,' using the evolving tactics of 'ambiguous war.' In the Third Offset Strategy the 'pace of change' is seen as a fundamental element in the security landscape. As Undersecretary for Defence Bob Work says in a speech on the strategy:

> Unlike the previous offsets, the fielding of tactical nuclear weapons and precision-guided bombs and missiles, which deterred war and gave the American military in some cases four decades of advantages over adversaries, this new technology probably won't provide an edge that long.(Work, 2015)

The anxiety is that all the 'traditional' hierarchies – the order that 'international society' upheld - is disrupted by the pace of change, a pace of change that provides dangerous opportunities for non-state actors and 'peer competitors.' According to Work, the potential to lose the competitive edge in technology stems *from* vulnerabilities in cyberspace: 'What's more, some of the potential competitors are letting us do the research and development, then they steal it from us through cyber theft and they go right to development, rather than spending their own resources on Research and Development (R&D)'(Ibid). On this view, the cyber threat becomes a danger through the way it impacts on traditional elements of defense and security.

Great powers/peer competitors play the biggest role in this visions of future insecurity. In 2013 a small independent ‘b’ movie (film and popular culture can a role in legitimating hypersecuritization) was released that depicted a cyberattack orchestrated by China on the critical infrastructure on the United States. The cyber attack was a reaction to the failure of the U.S. to pay back its debt. The Chinese are able to shut down critical infrastructure and invade the U.S: the movie becomes a 21st century version of the 1980s Cold War movie, *Red Dawn* that depicted young Americans resisting an occupying force from Russia. *Dragon Day* (Directed by Jeffrey Travis, 2014) built this scenario on the fear – a fear that we have seen circulate in real world discussions of cybersecurity - that some products ‘made in china’ may contain malware that can be activated to control/shut down the everyday technologies we use and the critical infrastructure that we depend upon.

While the movie might tap into and express broader fears about the rise of China, most commentators would see this type of cyberwar scenario as geopolitical science fiction. Most cyber catastrophists would agree with Thomas Rid that sabotage, espionage and subversion are the primary cyber tactics that states will develop and deploy (Rid, 2013). But where the ‘extrinsic catastrophist’ – those who argue threat comes from the outside - might differ with Rid is on the question of scale and destructiveness of new types of sabotage, espionage and subversion. The counter-argument to this catastrophist position is that a state will not launch such a cyber-event because they will face the same constraints and deterrents that would apply to more traditional weapons. But for the *extrinsic* catastrophist the issue is that the actions of deterritorialized and networked non-state actors won’t be shaped by the same anxieties about retaliation and laws of war that will shape the behaviour of states. In addition, there might be states that support non-state actors, enabling them to orchestrate the type of destructive events that previously only states could orchestrate: states that engage in such practices of ‘ambiguous war’ will be playing with fire. But for the extrinsic catastrophist the problem is that non-state actors might obtain the capability to act like states. Or even more troubling: an individual might obtain the destructive capacity of a state or non-state actor. We heard one expert refer to the possibility of the S.I.M.A.D – the single individual massively destructive.

For the cyber catastrophist the state is a realm of organised irresponsibility. For former National Coordinator for Security, Infrastructure Protection and Counterterrorism, Richard Clarke, we have to face the reality of possible cyber 9/11s or Pearl Harbors. For Clarke and Knake, we are moving headfirst into a more vulnerable and insecure security environment.

> The speed at which thousands of targets can be hit, almost anywhere in the world, brings with it the prospect of highly volatile crises. The force that prevented nuclear war, deterrence, does not work well in cyber war. The entire phenomenon of cyber war is shrouded in such government secrecy that it makes the Cold War look like a time of openness and transparency. The biggest secret in the world about cyber war may be that at the very same time the U.S. prepares for offensive cyber war, it is continuing policies

> that make it impossible to defend the nation effectively from cyber attack.(Clarke and Knake, 2010, p.xi)

At the same time, there are cyber catastrophists outside the realm of national security thinkers and experts. The influential French philosophers and social critics Jean Baudrillard and Paul Virilio wrote about technology and catastrophe since the 1960s from the perspective of 'intrinsic catastrophists': Virilio and Baudrillard are both concerned that progress *is* catastrophe in our accelerated times; catastrophe comes from the worlds we build. For Paul Virilio, the problem is the possibility of the integral accident (Virilio, 2007) The integral accident is the possibility of the accident that is magnified due to the interconnected nature of the world we live in: an example might be a financial crisis or the possibility of cascading global impacts that result from human-generated climate change. Our complex, interconnected world generates the possibility of accidents and disasters that are not confined to a locality – the local accident can become global and the impact of the local event can extend through time. Virilio suggests we are too seduced by the possibilities of transforming society offered by new technologies, the promise of speed, efficiency and networked existence. For Virilio, the problem is that we are designing and creating a fragile technological infrastructure that will exceed our capacity to control it. Jean Baudrillard adds this suggestion on the future of insecurity: in modernity we view history as a process that improves the human condition. But for Baudrillard, the pace of technological change now has the capacity to be too disruptive: the pace of change that we are witnessing in technology will lead to 'exponential instability' (Baudrillard, 1994, p.87). These are problems that reach beyond the problem of organized irresponsibility and failures of governance and regulation.

The cyber catastrophist suggests that while we need to be wary of inflated and unsupported threats the primary task here is take seriously the possibility of digital disasters and catastrophes – and to assess whether different organizations tasked with securing and protecting us are acting responsibly. While the digital disaster scenarios of movies like *Dragon Day* are geopolitical science fictions, we are seeing events that suggest that unprecedented cyber catastrophes could take place - but they wouldn't look like anything we can currently imagine in a world of 'exponential instability.' The question the catastrophist leaves us with: where are the vulnerabilities and what are we failing to see?

The Digital Realist

For the digital realist of cybersecurity and cyberwar, *Dragon Day* would be an example of the most extreme panic and paranoia in debates about cybersecurity. The digital realist is positioned as a counterpoint to the cyber catastrophist, arguing against the 'hype' of the catastrophist in the hypersecuritization of digital disaster and catastrophe. Visions of future catastrophic events – such as the attacks on transportation networks in London depicted in the James Bond film *Skyfall* (orchestrated by a 'foreigner' with a grudge against the UK) - create very marketable products in popular culture. There will also be those who benefit economically from the political economy of cyber security is created by new threats and insecurities. Indeed, one cybersecurity expert told us about how some organizations, businesses and parts of governments were becoming increasingly sceptical about some of the catastrophic scenarios that were used in the promotional material for the cyber solutions and tools that they wanted to sell. Like Hansen and Nissenbaum, the digital realist sees countering hypersecuritization as the primary task in this space; and this countering of hypersecuritization has become central to debates on cyberwar and cybersecurity.

Thomas Rid argues that it is highly problematic to talk about the possibility of cyber *war*. We are unlikely to be involved in conflict where a cyber instrument is the primary 'weapon.' War is the use of violence to achieve specific political or economic objectives through techniques that make the enemy defenceless. Even if it were possible to fight a war with cyber weapons they are unlikely to have the violent capability of more traditional weapons. According to Rid, what we are likely to see are cyber instruments used for espionage, sabotage and subversion.(see also Valeriano and Maness, 2015). It might be the case that subversion results in events the far more extreme than anything we have been used to, where, for example, an attempt is made by an external actor to shape the election campaign of another state. But we will become more prepared to counter such threats.

The realist would most likely support this point in the *Global Agenda 2030* report on the 'game-changing' potential of cyber as a weapon of war:

> The degree to which cyber instruments will shape the future of warfare is unclear, however. Historians of war believe cyberpower may end up somewhat akin to early 20th century projections of the decisiveness of air power. Although air power played a significant role in 20th-century conflicts, it never achieved what its most ardent enthusiasts claimed it would: an independent war-winning capability(National Intelligence Council, 2012, p.67).

But all this is not to say that cyber techniques of conflict, crime and disruption are not destructive to the national interest. But when we talk about the impact on the national interest and security, the consequences are generally not physical death and destruction. The key challenge for the military will be how to benefit from digitization in terms of speed, safety, efficiency and cost-effectiveness while not creating new types of vulnerability. But, at root, cyber is just another in a long list of problems that society confronts and much of the impact- the reason for it being a security threat – is the economic impact. In *Securing Britain in an Age of Uncertainty* the data to support the argument that cyber had become a threat to national security is all economic (The Cabinet Office, 2010).

All the problems associated with cyber are just nuisances in the lives of citizens, corporations and states. But they are nuisances that will often emerge from the territories in the non-West where governments are unable to govern – and maybe even encourage – criminal organizations able to exploit vulnerabilities in digital economies. A key 'villain' in reports of various cyber events – from the Sony hack to the Bangladesh Central Bank heist – is often North Korea, presented as a state that is so far out of the international system that it can use tactics that no one else would, willing to take risks no one else would. This representation of the geopolitics of cybersecurity might provide an ‘easy target’ through which to explain an emerging terrain that is far more diplomatically complex than can be revealed in the public sphere; a geopolitical terrain represented with a new generation of cyber ‘villains,’ often with ‘oriental’ cyberpunks and hackers depicted causing clever types of digital disruption, experts in the new techniques of corporate/military espionage, a trope that we find in cult cyberpunk such as *Ghost in the Shell* through to mainstream movies such as Christopher Nolan’s *Inception*.

But for the digital realist, cyber is a twenty first century *nuisance*- and a relatively minor one compared to the benefits that digital technologies provide in our lives and economies. Cyber will play a role in the security landscape we will be confronted with but we should not overstate the cyber element. Our virtual territories of data and intellectual property might be under attack but the type of scenario depicted by *Dragon Day* is not going to happen. Putting to one side the issue whether it would be even possible to shut down the United States *remotely*, it is not going to happen for the same reason that great power conflict becomes less likely: the threat that traditional weapons of mass destruction will be used. There would have to be a severe degradation of the international ‘scene’ for traditional territorial war between great powers to return and if the degradation of the terrain reached such a critical point it is unlikely that cyberweapons would play a decisive role.

Of course, one of the arguments in this terrain is that in the coming century non-state actors will be empowered in new ways. But, for the digital realist, it is unlikely to get to the point where they could do anything significant: critical infrastructures are too resilient (Calvety 2008, p.139); states will retain the monopoly over violence and weapons of mass destruction (and the monopoly of cyber offensive and defensive capability). Some might argue that the cyber weapons that states have deployed – such as Stuxnet – will be developed and used by non-state actors. But malware like Stuxnet are expensive to develop and require long term planning and research, with a high level of access to information about the infrastructure that will be attacked (Singer and Friedman, 2013). Malware like Stuxnet are state of the art projects by the most powerful actors in the international system and even if non-state actors develop similar projects in coming decades they will have to deal with the fact that there will be increased research and development in the protection of systems. Of course, there could be well funded research facilities in shadow economies and failed states but there are less sophisticated ways of making money or making a political point. As Myriam Dunn Calvety suggests: ‘These doomsday scenarios are quite frightening. But it is good to know that they are about as likely to happen as a landing of alien spaceships’ (Calvety, 2011).

The digital realist would argue that we should continue to focus on the development of offensive and defensive cybersecurity and cyberwar strategies. But we need to be careful not to equate cyberweapons with ‘game changers’ that will transform the future of war and create the possibility for destructive scenarios common in science fiction movies. On this view, there will always be technical fixes to secure critical infrastructures; non-state (and non-West) actors will lack the capability and states – even if they could – would lack the incentive to create a cyber-catastrophe that resulted in ‘physical’ violence.

We have to recognize that there are limits to what we can do: cyberspace is only partly controlled or controllable by governments. For the digital realist, it all comes back to the problem of resources. We do not want to over-react in our response to threats with costly measures and uncertain benefits, leaving government with less for middle to low impact but high probability threats (Calvety, 2008, P.151). Like Hansen and Nissenbaum, the digital realist suggests that we need to counter hypersecuritizations, remaining alert to the possibility that the conditions of cyberwar may change – but for now are Twenty First Century nuisances with primarily social and economic consequences. The questions the digital realist leaves us with are: how can we avoid exaggerating the threat of cyber war – and how (for the more 'strategically' minded) can we use these new techniques and technologies to 'improve' performance in our traditional militaries *without* creating new vulnerabilities?

The Techno Optimist

Rejecting the pessimism of thinkers like Virilio and Baudrillard, the techno-optimist views History as a story of Progress. Improvement in the human condition is primarily driven by the emergence of liberal democracy – where despotic power is limited by the will of the people and where 'tribal' identities are overtaken by more expansive and potentially cosmopolitan ones – and by the emergence of new technologies that improve health, communication, economy and security. Societies are transformed by changing values, norms and institutions that move toward the inclusion of those who would previously been seen as inferior and through laws that protect human rights (Pinker 2012). The techno-optimist believes that if societies develop the right type of institutions and political culture we can continue the process of overcoming the catastrophes and dangers of the human condition. The liberal democratic world is not perfect: things go wrong, mistakes are made - but liberal societies have mechanisms of critique and reflection that enable learning and improvement. This is part of the resilience of liberal democracy.

Writing about what he terms 'protopia,' Kevin Kelly (one of the leading 'thought leaders' on new technology and the impact on society) suggests that 'neither dystopia or utopia is our destination': 'Protopia is a state of becoming, rather than a destination. It is a process. In the protopian mode, things are better today than they were yesterday, although only a little better' (Kelly, 2016, p.13). The techno-optimism of this 'protopia' rests on the view that:

> The problems of today were caused by yesterday's technological successes, and the technological solutions to today's problems will cause the problems of tomorrow. The circular expansion of both problems and solutions hides a steady accumulation of small net benefits over time. Ever since the Enlightenment and the invention of science we've managed to create a tiny bit more than we've destroyed each year (Ibid, p.13).

Kelly suggests that while there is clearly the potential for catastrophic events emerging from new technology, we should recognize that in the 'protopia' this 'circle of new good provoking new bad which provokes new good which spawns new bad is just spinning us in place, only faster and faster' (Ibid, p.275).

For the techno-optimist (or protopian) there will be accidents and disasters but they will not have the impact of the worst-case scenarios of the hypersecuritizer; and in the 'protopia' we will build capacity in response to vulnerabilities and dangers; we will reduce the dangers in times when the digitization of all aspects of life will exceed anything we can imagine. For the techno optimist, what we need to be doing is focusing on research and education; we need, for example, to be supporting research that will provide the technical fixes to fight the insecurities of the digital age: we need to be training the next generation of cybersecurity experts to help secure individuals, corporations, states and the military. Most cyber 'catastrophes' result from errors or sloppiness that will be easy to rectify: for example, an attempt to make fraudulent transfers totalling $951million after cyber criminals hacked Bangladesh Bank in 2016 was possible due to the lack of a Firewall (and the bank used second hand $10 switches to connect to the SWIFT global payment network) (Quadir, 2016). An international legal architecture will emerge to control and shape the behaviour of states and non-state actors in cyberspace; we might be experiencing a moment when our technology is leading us into unchartered and ambiguous terrain but we will becoming better at making sure law and global governance keeps up with the pace of change.

In terms of cybersecurity and cyberwar, the techno-optimist is enthusiastic about the digital age. The risk of cyber catastrophes on the threat horizon will be eradicated by the technological solutions produced by artificial intelligence and better ways of spotting vulnerabilities, the 'glitches' in code that create unintended consequences (Vatamunu, 2016). The primary fear is not about future cyberwar or cyber catastrophes but on the way that states will use new technology for surveillance and the control of populations. The techno-optimist is primarily concerned with the militarization or 'Balkanization' of the internet: the techno-optimist sees the global community that exists on the internet as one of the most important and positive aspects of digital culture. But one of the problems for the techno-optimist is how liberal, progressive ideas can spread in the territories that cultivate authoritarian political structures. The ideal scenario for the techno optimist is for political change to emerge peacefully from the 'bottom-up': the techno optimist is concerned that – after some initial post-Cold War optimism about the future of liberal democracy – we live in a world where authoritarian regimes seem to be in good health, balancing dynamic economies with authoritarian political cultures. The anxiety here is that the hypersecuritizing obsessions of the state turns inwards, using new innovations to monitor and police populations; and in the debates on security in the 'non-West' there is a concern about the *Minority Report*-like futures that will be possible in a way that is unlikely to materialise in a West anxious about privacy and civil liberties (although this could change – and perhaps is already changing – driven by hypersecuritized anxieties).

The possibilities of positive cultural and political change are even weaker if the internet is militarized or Balkanized: the possibility of grassroots communication, education and mobilization becomes limited. For example, in July 2014 the Russian Parliament passed a bill requiring all technology companies to store the personal data of all their users in the country; coming into effect in September 2016, the policy was justified in terms of national security. It was the first serious step to assert national control over segments of the web in light of the revelations about the surveillance by the US National Security Agency; Russia's internet regulator had complained about the lack of cooperation from tech companies like Google, Facebook and Twitter in blocking content deemed illegal by the state (Hills, 2014). A fragmented internet-moves from being a potential space of freedom to a tightly controlled 'shopping mall' developing new and improved techniques to sell 'stuff' and monitor populations. There will be those who can by-pass these controls. But these numbers will be small; the possibility for popular resistance will be limited. For the techno-optimist, the global politics of cybersecurity should be focused on protecting the cybersecurity of the citizen against a hypersecuritized threat horizon shaped by states and their new everyday security practices.

The digital realist would most likely remain cautious about the faith in new technology to transform war into something more humane: the techno-optimist will see positive 'protopian' developments in the waging of war. On this view, military technology is moving in a direction that reduces the risks faced by the soldiers of liberal democracy – and the precision of weapons creates less collateral damage on civilians close to the targets. This trend toward more humane forms of war will increase and the evolution of malware like Stuxnet will create a new generation of digital weapons (Coker, 2001). States will be able to use 'information bombs' that will destroy the technological infrastructure of city or town without killing human beings – but forcing change in the behaviour of opponents. Of course, there are those (the catastrophists) who argue that we are entering an age where far from making war more humane and controlled technology is creating a type of war that will be fought be machines and artificial intelligence that will have the power to decide who lives and dies. But the techno-optimist will reply that liberal democracies will continue to impose limits on what is permissible. Our culture of human rights means that there is a great deal that is possible in terms of military technology that simply will not be realized – at least by liberal democracies (what China and other states build is another matter) - and we will always place legal constraints on what is permissible in war. The trend in military technology is not toward automated killing machines but toward smart cyber weapons that *enable destruction without destruction*, 'novel munitions,' non-lethal weapons and *incapacitators* that will create 'bloodless' war.

For the techno-realist, the task is to counter – in particular – the securitization of everyday life, the invocation of threats – domestic or foreign – to justify new measures to regulate people's digital lives and to justify the introduction of new tactics and technologies to regulate all aspects of everyday life. This is, in many ways, the concern Hansen and Nissenbaum articulate on how computer scientists might become 'more cognizant of the politicized field in which they design and how their decisions might impact the (discursively constituted) trade-offs between security, access, trust, and privacy.' The question the techno-optimist leaves is with is – how do we resist attempts to limit the freedom of our digital lives and where are the innovations that will transform conflict in the coming century?

Concluding Remarks: Granular Security and the Geographies of Cybersecurity

Since the publication of the essay by Hansen and Nissenbaum in 2009 attempts to counter the hypersecuritzation of cybersecurity and cyberwar have intensified – from a variety of perspectives and theoretical backgrounds (the most notable being Thomas Rids *Cyberwar Will Not Take Place* and Rid's debate with John Arquilla) (Arquilla, 2012). What we outline in this paper are what we see as the three key positions on cybersecurity and cyberwar that are currently central to the debates circulating in this emerging terrain: the cyber-catastrophist, the digital realist and the techno-optimist. Here we are trying to go beyond the framing of the cyber debate in terms of cyberwar will take place (and it might be as destructive as traditional war) and cyberwar will not happen (it will involve new tools for older techniques of statecraft). We are suggesting that while the debates that have been waged on the changing character of cyberwar have been vital in clarifying the issues at stake we need to remain open to the possibilities revealed in each position. This openness needs to be maintained exactly because of the – to use some U.S. military jargon - VUCA (Volatile, uncertain, complex, ambiguous) nature of things at this point in time: the extremes of these positions might veer into geopolitical science fiction but the questions each position poses are important ones and questions that will grow in significance exactly because of the pace of geopolitical and technological change; we need to move between them, constantly re-examining the key questions and assumptions as the 'terrain' changes (and as new questions and positions undoubtedly emerge).

In particular, we are suggesting that – while the point that Hansen and Nissenbaum conclude with on the need to be able to counter hypersecuritization and technification remains the key issue here - we need also to examine what questions and concerns are sidelined *in* the zones of technification. What we have found talking to cybersecurity professionals working in a variety of organizations is that many would see an importance in the questions and concerns of each perspective; we heard one expert say that they felt like a catastrophist working in organization x and an optimist working in organization y. One cyber 'expert' from the military world remarked to us that 'in cyber the one eyed man is king.' In 2017, for example, it was reported that National Health Service (NHS) Trusts were left vulnerable to Ransomware attacks in May of that year because cyber-security recommendations were not followed (Cellan-Jones, 2017). While these events may not be described as 'catastrophic' (6,900 appointments were cancelled) the question is clearly about future catastrophic events and the organised irresponsibility that may neglect or ignore certain vulnerabilities: in the organisations that are shaping the future elements in the security and military apparatus there may be failures of imagination on future threats or the digital disasters (or 'integral accidents') that may emerge from the environments that are being designed.

The problem of technification is not simply on how it might add legitimacy to hypersecuritization, in what it enables us to visualize in the imagination of digital disaster – it is what it fails to see or ignores. This risk might intensify in a time when a variety of actors are shaping the digital worlds we inhabit. Or put another way: we need to assess the possibility is that there is a problem of 'desecuritization' in the zones of technification: we need to consider the possibility that organizations that play important roles in all areas and elements in security and war might fail to examine vulnerabilities in the race for efficiency, speed and cost-effectiveness. On this view, we need to examine how cyber securitizations move from the political into the technified but also how issues and concerns can be erased – or desecuritized – through the dominance of a particular group or mindset *inside* the zones of technification. These concerns may be overstated – maybe 'organized irresponsibility' is an ungrounded fear- but these are questions that require attention.

But another trend is clearer now than it perhaps was in 2009. Thinking about the various problems/levels of cybersecurity – from the everyday and individual, the critical infrastructures of national security, the corporate and economic – in the context of securitization and the 'non-West' raises a number of issues. Securitization theory – and poststructuralist work in global politics – is interested in how 'otherness' and 'difference' circulate in (and are fundamental to) broader discourses of geopolitics and international relations; in this sense, discourses of cybersecurity – and the positions outlined in this essay – contain various types of digital danger emerging from the 'non-West': terrorists using the internet for radicalisation, devious hackers from North Korea, hi-tech techniques of surveillance in China. But thinking about cybersecurity issues in terms of traditional geopolitical categories – developed/ developing, and so on – begins to look problematic in a world where all territories are being transformed by new technologies and where the sources of vulnerability become *deterritorialized*: threats can come from a 'problematic' zone of global politics but it might also come from a bedroom in the same town in your 'safe European home.' Innovations in technologies (and new uses of existing technologies) might continue to emerge from California and Silicon Valley – but they might also emerge in states anywhere around the planet.

Securitization theory warns us to be careful about the ways in which otherness can be drawn into broader geopolitical discourses of danger and difference. But what it can also alert us to is the tendency to write over the complexity and messiness of events and developments in global politics with visions of security and geopolitics that ignore the specific and particular characteristics of the worlds that are being researched and written about (see Hansen 2006). Hansen and Nissenbaum's essay is a call to explore the complexity of cyber, to think more critically about what constitutes a catastrophe or digital disaster and the different problems that can be absorbed into the discourses of hypersecuritized threat. But what is clearer now is the need to explore the complexity of cybersecurity in different geopolitical and economic contexts around the planet, to become *granular* in our analyses, to explore the possibility that – while many cyber events emerge from the entangled, interconnected nature of events in the Twenty First Century – there may also be new trends and developments in the ways that new technologies are used (and abused) in different contexts, to examine the new everyday security practices that might be experimented with in different states, to examine the specific vulnerabilities that might be emerging for individuals and communities in different places around the world. From the conflict over bloggers in Bangladesh, to the everyday security practices that Chinese citizens live with, to new types of crime in sub-Saharan African states, to the use of new technologies by Mexican drug cartels, new research on the global poltics of cybersecurity needs to examine the local complexities and challenges faced not simply by states and corporations (the standard, 'official' approach to cybersecurity) but also by individuals and communities (the move that securitization theory prompts us to take), examining the tactics of states and non-state actors using digital strategies and techniques. The three positions outlined here can begin to open research questions to begin to examine the *glocal* contexts of cybersecurity and the various issues and challenges of securitization:

> The Catastrophist: here the problems is to examine the potential for accidents and vulnerabilities (and what Rid would see as sabotage) – ranging from the relatively local and manageable to the more national and potentially catastrophic – that might emerge from the particular legal, political, economic and technological context; to examine the political and legal processes of technification that securitize issues or leave them in the realm of organised irresponsibility; to explore new types of crime that are possible due to trends in economy and technology (such as problems with 'mobile money' in states like Ghana or Nigeria, or new techniques of political and economic corruption).
>
> The Techno Optimist: the problem is to explore the legal and political pressures that are attempting to shape the digital lives of citizens; to examine the techniques that might be used against the 'internal' others through new technologies of surveillance or abuse/harm; to examine how violence and conflict is being transformed through new technologies (see, for example, Narrain, 2017); to examine emerging tactics and trends that may be 'globalised' as useful techniques by states seeking to manage what they see as a the problematic digital 'mob'; or to examine new techniques of subversion that set out to shape the political landscape; and to explore the new possibilities for conflict prevention and resolution.
>
> The Digital Realist: the challenge is to see how militaries around the planet – even the military forces that would be viewed as relatively 'undeveloped' and minor – are envisaging the use of new digital techniques technologies; to examine how they are dealing with the problems that - while not potentially 'catastrophic' – may result in operational and organisational problems (espionage, subversion minor accidents or sabotage that may impact the functioning of an organisation).

So we need to remain open to what is happening in the digital lives of others, to the new vulnerabilities they confront, to the new forms of control that are deployed against them, to examine the trends in territories that might get ignored in our (imaginary) maps of digital geopolitics. But in the process of 'globalising' these research questions, we should not lose sight of the need to think about the organised irresponsibility that we might find in the organisations and institutions that pride themselves as being the most 'advanced,' 'rational' and 'cutting edge.'

Bibliography

John Arquilla (2012) 'Think Again: Cyberwar', *Foreign Affairs*, 27th February: http://foreignpolicy.com/2012/02/27/think-again-cyberwar/

Thierry Balzacq (ed) (2011) *Securitization Theory: How Security Problems Emerge and Dissolve* (London: Routledge).

Jean Baudrillard (1994)*The Illusion of the End* (Cambridge: Polity).

Ulrich Beck (1999) *World Risk Society* (Cambridge: Polity)

Myriam Dunn Calvety (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information* Age (London: Routledge).

Myriam Dunn Calvety, 'As Likely as a Visit from E.T,' *The European*, 07.01.2011: http://www.theeuropean-magazine.com/133-cavelty/134-cyberwar-and-cyberfear

Rory Cellan-Jones (2017) 'NHS 'could have prevented' Wannacry ransomware attack,' *BBC NEWS*, 27 October 2017: http://www.bbc.co.uk/news/technology-41753022

Richard Clarke and Robert Knake (2010) *Cyberwar: The Next Threat to National Security and What to do About It* (New York: Ecco).

Christopher Coker (2001) *Humane Warfare* (London: Routledge).

Lene Hansen (2006) *Security As Practice: Discourse Analysis and the Bosnian War* (London: Routledge).

Lene Hansen and Helen Nissenbaum (2009) 'Digital Disaster, Cyber Security, and the Copenhagen School,' *International Studies Quarterly*, 53, 1155-1175.

Kathrin Hills (2014) 'Russian move to control data stokes fears of the Balkanisation of the internet ', *Financial Times Weekend*, Saturday July 5/6, p.10

Kevin Kelly (2016) *The Inevitable* (New York, Viking).

Siddharth Narrain (2017) 'Dangerous Speech in Real Time: Social Media, Policing, and Communal Violence,' *Economic and Political Weekly: Engage*, 24 August: http://www.epw.in/engage/article/dangerous-speech-real-time-social-media-policing-and-communal-violence?0=ip_login_no_cache%3Da2d514cacfc04ca25be50c2bb148a93c

National Intelligence Council (2012) *Global Trends 2030: Alternative Worlds* : https://globaltrends2030.files.wordpress.com/2012/11/global-trends-2030-november2012.pdf

Steven Pinkers (2012) *The Better Angels of Our Nature* (New York: Allen Lane).

Serajul Quadir (2016) 'Bangladesh Bank exposed to hackers by cheap switches, no firewall: police,' *Reuters*, April 22nd : http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0XI1UO

Thomas Rid (2013) *Cyberwar Will Not Take Place* (London: Hurst).

Peter W. Singer and Allen Friedman (2013) *Cyberwar and Cybersecurity: What Everyone Needs to Know* (Oxford, Oxford University Press).

The Cabinet Office (2010) *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*.

Kim Zetter (2016a) ‘Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid,’ Wired, 03/03/2016: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

- (2016b) ‘That Insane, $81 million Bangladesh Bank Heist? Heres What we Know,’ *Wired*, 05/17/2016 :https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

Brandon Valeriano and Ryan Maness (2015) *Cyberwar versus Cyber realities* (Oxford: Oxford University Press)

Cristina Vatamunu (2016) ‘Outnumbered, yet strong: Artificial Intelligence as a Force Multiplier in Cybersecurity,’ *Bitdefende*r, July 12: http://businessinsights.bitdefender.com/artificial-intelligence-cyber-security

Paul Virilio (2007) *The Original Accident* (Cambridge: Polity).

Bob Work (2015) ‘The Third U.S. Offset Strategy and Its implications for partners an allies,’ 28 January, 2015: https://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies.