Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Desecuritising cybersecurity: towards a societal approach

Joe Burton & Clare Lain

To cite this article: Joe Burton & Clare Lain (2020): Desecuritising cybersecurity: towards a societal approach, Journal of Cyber Policy, DOI: 10.1080/23738871.2020.1856903

To link to this article: https://doi.org/10.1080/23738871.2020.1856903

Published online: 14 Dec 2020.

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2020.1856903

Routledge
Taylor & Francis Group

Desecuritising cybersecurity: towards a societal approach

Joe Burton[a,b] and Clare Lain[c]

[a]Recherche et Études en Politique Internationale (REPI), Université libre de Bruxelles, Bruxelles, Belgium; [b]New Zealand Institute for Security and Crime Science (NZISCS), University of Waikato, Hamilton, New Zealand; [c]Head of International Bodies and Technical Engagement, UK Hydrographic Office, Taunton, UK

ABSTRACT

Cybersecurity is often treated as a national security issue with responses to attacks implemented by military and intelligence agencies. This has created path dependencies in which tensions between the private sector and government have continued, where over-classification of cyberthreats has occurred, and where the broader societal impacts of malicious use of the internet have been underestimated. Drawing on the societal security concept established by the Copenhagen School of International Relations, we seek to reframe cybersecurity theory and policy. In the first section of the article we establish a theoretical approach to cybersecurity that emphasises the impact of cyberattacks on society, including on the health, energy and transport sectors. The second section draws on the history of cyberconflict to assess the ways the internet has been used to exacerbate societal tensions between identity groups and to create incohesion and societal security dilemmas. This section reinterprets the way the Kosovo War, Millennium (Y2 K) Bug, 9/11 and the WannaCry incident shaped and reflected cyber policy. The final section explores how a process of cyber desecuritisation might be achieved, including through discursive change and an enhanced role for the societal sector in the event of major cyberattacks.

ARTICLE HISTORY
Received 3 June 2020
Revised 1 October 2020
Accepted 26 October 2020

KEYWORDS
Cybersecurity; societal security; desecuritisation

Introduction

At the end of the Cold War, scholars and policymakers attempted to reframe security to better fit a globalising and complexifying security environment. The features of this environment included a transition away from bipolarity, the rise of identity-based intra-state conflicts, and the accelerating influence of information and communications technologies, most notably the internet. There was a considerable degree of inertia entering this new period between the policies and strategic thinking that dominated during the Cold War, including a fixation on interstate conflict and national security, and the demands of the new era. As cybersecurity concerns intensified around the millennium, most notably due to the Y2K bug, the advent of cyberattacks during the conflict in Kosovo and the subsequent fears that emerged over terrorist use of the internet and

CONTACT Joe Burton joe.burton@waikato.ac.nz

cyberterrorism in the post 9/11 environment, the need to formulate urgent solutions to cybersecurity challenges became more apparent. In addressing these problems, policymakers fell back on outdated Cold War concepts and approaches that were not the best fit for the emergence of a globally linked network of computer systems inherently vulnerable to exploitation.

Now, in many countries, including all the 'great powers' (the US, Russia and China), military and intelligence agencies have acquired a prominent role in cybersecurity. Offence is widely seen as providing the best defence in cyberspace, despite credible arguments to the contrary (Slayton 2017; Valeriano and Jensen 2019), and the cyber deterrence debate has been one of the central features of cyber theorising (Stevens 2012), even though, in its traditional form, the deterrence concept is ill-suited to contemporary cybersecurity challenges. This national, military and intelligence-agency-led approach to cybersecurity has been widespread, and has had several negative consequences for dealing with cybersecurity threats, including creating path dependencies in which tensions between the private sector and government have continued (Carr 2016), where overclassification of cyberthreats has occurred (Janofsky 2018), and where the broader societal impacts of malicious use of the internet are only beginning to be identified (Agrafiotis et al. 2018). In the emerging cybersecurity environment, states have reached out to control what they fear from the internet (Demchak and Dombrowski 2011, 36) and in doing so, have exacerbated many of the issues they were intending to address.

In this article, we seek to address these issues by proposing a move towards a societal security-based approach to cyber theory and policy. We argue that the societal security concept, which first emerged in the aftermath of the Cold War, is a better theoretical fit for cybersecurity concerns than traditional national security models, and that much of the malicious cyber activity over the last decade, including cyberespionage, cyber coercion, cyber and information warfare, and the subversion of social media, has been targeted at, and caused by, societal tensions. Focusing on societal cybersecurity, we argue, will help sectors where much of the impact of cyberattacks lies, including in health, energy, transport, finance and democratic governance (Oskui 2018) and will help to enhance societal resilience against cyberattacks. In building this argument, we draw on the existing literature on societal security and securitisation and apply the concepts to cybersecurity issues. As well as operationalising the societal security concept to address new cyberthreats, we make two other theoretical and policy-related contributions. The first is to seek to refine societal security theory by considering the sociopsychological effects of cyber activity. This additional cognitive layer, we argue, is important in understanding contemporary cybersecurity threats and policy. The second is to consider how a process of cyber desecuritisation might occur, a process, we argue, which is integral to moving away from the overly centralised and militarised approaches to cybersecurity that currently dominate the field.

The article proceeds in three main sections. The first section examines the concept of societal security, identifies its key components, relates these to cybersecurity challenges and supplements the societal security approach with a cognitive layer of analysis. In section two, we historicise key events in the emergence of post-Cold War cyberconflict and doctrine, including the Kosovo War, the Millennium (Y2K) Bug, 9/11 and the WannaCry event. We use these events as snapshots in the securitisation process and reinterpret them through the societal security lens. This section argues that a process of securitisation

was catalysed in the late 1990s and early 2000s that centralised and nationalised cybersecurity responses and created path dependencies that ultimately limited the ability of states to respond to cyberattacks. The final section of the article examines how policy could be reformulated to more effectively respond to cybersecurity challenges. In this section, we highlight pathways to cyber desecuritisation and argue that a continued predisposition to view cybersecurity through a national and military security lens will lead to a more unstable and uncertain global cybersecurity environment.

Societal security and cyberthreats

The societal security approach emerged in the early post-Cold War period as an alternative to strategic thinking and decision-making that had been dominated by the concepts of national and military security. Its most prominent theorist and proponent was Barry Buzan, whose writings contributed to the emergence of the Copenhagen School of International Relations. In a series of analyses in the 1990s, Buzan conceptualised the emerging security environment as consisting of five security sectors: military security, political security, societal security, economic security and environmental security (Buzan 1997). Buzan's approach reflected the emerging reality of the new era, where a rapid deterioration in societal cohesion in nations that had been held together by Cold War dynamics (such as in Bosnia and Kosovo) caused violence and regional instability. In this emerging, globalising security environment, Buzan argued, threats to nation states and peoples were increasingly from non-military means, including financial pressures, the environment, political instability and non-state actors, including terrorist groups. In delineating this new framework for analysis, Buzan recognised that the Cold War did not herald the end of military threats and interstate conflict and that these would continue to be a feature of the contemporary security environment. Non-military threats to security would likely take precedence, however, and he argued that the security studies discipline should broaden its focus to a wider range of actors and processes. The levels of analysis that had dominated International Relations (IR) thinking, moreover, which had largely been constructed around a division between the domestic sphere, state and international system, appeared to be outdated. A commitment to 'national security' and the relentless pursuit of national interests encouraged a militarised approach to security, drove security dilemmas and contributed to economic and military dislocation. National security, Buzan noted, was almost a contradiction in terms (29).

The societal sector was a major focus for Buzan within this framework and was concerned with the collective identity of peoples within states in a period in which the concept and role of the state was under threat. 'International' security, Buzan argued, contrary to the prevailing wisdom, 'was mostly about how human collectivities relate to each other in terms of threats and vulnerabilities' (Buzan 1997, 10). These collective identities could either operate independently of the state or be shaped by the interrelationship between state and society. They evolved over time, and were threatened by both *internal* and *external* factors, including fears that groups were losing their identity because of persecution by states, and globalised issues, such as migration and transnational crime. The societal security approach referred to 'the ability of a society to persist in its essential character under changing conditions and possible or actual threats' (23) and assumed that states and societies were not separate but mutually constituted.

To date, there have been relatively few societal security-based analyses of cybersecurity issues (see Hansen and Nissenbaum 2009; Gioe, Goodman, and Wanless 2019). Much more analysis has taken place in the fields of terrorism, migration, environmental scarcity and intra-state conflicts. Despite this, the societal security approach has obvious salience for the analysis of cyberthreats.

First and foremost, cyberattacks have been caused by, and used strategically to exacerbate, social and political tensions between identity groups. A commonly cited example was the dispute between the Estonian state and Russian hackers in response to the 2007 'Bronze Soldier' incident. This was a major event in the evolution of cybersecurity in the post-Cold War era and was founded on tensions over Russian influence in the Baltics, including identity-based, cultural and historic divisions between the Russian-speaking minority and non-Russian Estonians. In line with the theoretical parameters of the societal security approach (Bilgin 2003), the attacks were both a symptom of societal divisions and served to exacerbate and highlight them. They were also influenced by a variety of socio-psychological dynamics, including the loss of status of Estonia's ethnic Russian minority; the anonymity and depersonalisation coming from online interaction; group membership and adherence to group norms; and contagion through online forums (Guadagno, Cialdini, and Evron 2010). Despite this, the attacks were framed as nationally-oriented, with Estonian leaders evoking nationalised rhetoric – a 'blockade' – to describe a transnational computer network-based intrusion (Rid 2012).

As well as exacerbating tensions within societies, cyberattacks have exacerbated tensions *between* societies. This applies to the Estonian case and many others. As per the societal security framework's central premises, interstate relations (between governments, ostensibly) are not always the 'referent object' of analysis. Social, ethnic, religious and national groupings beneath the state level constitute independent actors and can be threatened, both across state boundaries and from within the state, by other groups or their governments. In this scenario, a 'societal security dilemma' may emerge, where efforts to harm an identity group may lead to that group using military or non-military means to defend itself (Roe 2004). Such societal security dilemmas can be compounded by new technologies, as well as potentially being alleviated by them. While there are relatively few examples of persecuted groups responding to insecurity through cyber operations, the emergence of 'privateers' in cyberspace would appear to fit this theoretical supposition. Chinese nationalists, for example, have used cyberattacks to respond to transnational disputes over territorial claims in the South and East China Seas, and hackers in the Philippines, among others, have retaliated in kind (Muncaster 2012). Perceiving their nationality and identity to have been questioned, these groups of hackers form complex social networks that are relatively unconstrained by bureaucratic, state-based operating procedures or international norms. In this sense, cyberconflict has emerged as an ostensibly social phenomenon, populated by a diverse range of social actors and movements, including patriot hackers, cyber jihadists, and other religious groups (Denning 2011). In the Chinese case, hackers have formed independent communities, cultures and hierarchies within Chinese cyberspace and are seen as both a threat to the Chinese government and a tool of it (Hang 2014).

The societal security approach also recognised that the security of societal groups could be threatened from other security sectors. These military, political, environmental and/or economic threats could 'spill over' into the societal sector (and vice versa) and

operate on a cross-sectoral basis (Roe 2004 , 57). In the most comprehensive application of Copenhagen School principles to cybersecurity, Hansen and Nissenbaum argue that it is plausible to think about cybersecurity as a sector of its own, and one that underpins the other sectors (Hansen and Nissenbaum 2009). Military investment in cyber capabilities, regime threats stemming from cyberspace, and the economic impact of cyberattacks, all suggest cross-sectoral relevance and important state-society dynamics. Environmental analogies have also often been used to explain cyber issues, including the notion of a cyber commons and more negative characterisations of global meltdown of infrastructure akin to extreme climactic events. The view of cybersecurity as insulated from other sectors of security, a position initially maintained by Copenhagen School scholars themselves (Buzan 2007; Hansen and Nissenbaum 2009, 1156), appears to be increasingly untenable. There have been various historical examples of military and intelligence-led cyber operations spilling into the societal realm. The use of the Stuxnet virus had considerable collateral effects, for example (Carr 2010), including self-replicating, being released on the internet, being reverse engineered (variants are still in use today) and acting as catalyst for the development of Iran's own offensive cyber capabilities (Black 2012). The Sony Pictures Hack in 2014 could also be seen in this context. The dispute between the North Korean regime and the US government over the release of the film *The Interview* had societal effects in the US, including the cancellation of the film's release and a debate about free speech. But it was caused by, and deeply connected to, a historical and ongoing dispute between the US and North Korean governments. In line with the societal security framework, the film itself was perceived to be an insult and challenge to North Korea's identity and culture and resulted in securitising rhetoric that intensified geopolitical tensions between the two powers.

Society, the state and market consolidation

The theoretical flexibility of the societal security concept moved the IR discipline away from traditional security actors and processes at the state level. During the Cold War period, the creation of powerful national security apparatuses in major states led to security monopolies forming, where governmental actors controlled the processes of security and accumulated considerable bureaucratic and political power. Buzan's analysis, along with others, is predicated on the notion that power has been diffusing away from state structures to other actors within society. The state itself has become permeable, increasingly unable to provide security for its citizens according to traditional structures and expectations, and the societal sector has risen in importance. This is not to say that states were 'withering away', as the Marxist framework would suggest, but that their authority, legitimacy and capability to deal with emerging security issues was increasingly challenged. States exercise considerable control over digital infrastructure, especially in countries where the approach to internet governance is more centralised, where censorship exists, and where internet and privacy freedoms are not enshrined in law. However, in advanced western democracies, security is increasingly contingent on the internet service providers themselves, social media platforms and critical infrastructure operators.

Fundamental to these emerging dynamics was the consolidation of the internet industry itself, and the emerging domination of a few key players, most notably Microsoft, Google, Facebook and Apple. This consolidation introduced a number of dynamics into

the state-society relationship, which, arguably, did not help cybersecurity. These included governments not wanting to regulate the ICT sector, either because of desires to have 'small state', 'light-touch' regulatory frameworks or because of the power of these companies to influence policy, and the fact that the large platforms acted as magnets for malicious activity and attacks against them which created outsized, system-wide risks (Geer et al. 2020). While the internet emerged as a platform for information sharing and transparency, two dynamics and processes that can mitigate misperception and mistrust, it also became a threat to regime stability and security. The spread of disinformation and misinformation, fake news and the emergence of internet-based social networks resilient to objective truths (climate change deniers for example), has certainly exacerbated the societal tensions that societal security scholars identified and about which they were concerned. More specifically, market concentration affected states' ability to manage and respond to cyber crises and major incidents, as will be explored later in this article.

Societal security and the cognitive turn

The latest research on societal influences on cybersecurity supplement these theoretical assumptions by elevating the cognitive influence of cyberattacks and the cognitive effects generated within target populations. Fear, uncertainty and the sense of anxiety that cyber intrusions engender may shape responses in irrational ways, including in a national security context (Gomez and Villar 2018). There is a growing body of literature that suggests cyber operations can influence political opinion and the psychology and behaviour of people and groups. In one recent analysis of the cognitive influence by cyber operations, Gomez and Villar (2018) found that cyberattacks cause apprehension among the public and that cyber decision makers often base their responses to cyberattacks on false assumptions influenced by narratives and the framing of cyber events, such as 'digital pearl harbour'. As Branch (2020) has recently argued, the use of these types of metaphors – including recent references to cyber as a 'domain' of war fighting – has been consistent throughout the post-Cold War period and influential in policy processes, including shaping the formation of the US Cyber Command and subsequent efforts to replicate the US approach to cyberwarfare by other states. In this way, metaphors become part of mental maps or cognitive schemas (Bloomfield 2012, 452), which influence policy.

Efforts to reduce bias in decision-making on cyber are also influenced by a lack of transparency and information sharing, especially within and between national security structures (Gomez and Villar 2018). Decision-making is also affected by the emotions of decision makers. As McDermott (2019) argues, fear and anxiety create moods, stress, fatigue and time pressures, all of which can adversely shape cyber policy, and can be manipulated by hostile actors. Social context also influences how cybersecurity attacks are responded to and interpreted. National security apparatuses tend to see the world in a certain way, may privilege military responses over diplomatic ones, tend to interpret espionage as an attack and may misinterpret the intentions of other states (Brantly 2016). As we go on to argue, these psychological and strategic cultural dynamics have been at least partly responsible for the centralisation of cyber responsibility within national security apparatus, and the problems that have resulted, including the intensification of societal security dilemmas.

When these cognitive and emotions-based dynamics are scaled to apply not just to individual leaders, but societies and the groups within them, the relevance and impact of societal insecurity becomes even more apparent. Recent events, including Russian influence operations in the US elections and Brexit, as well as the Cambridge Analytica scandal, provide evidence of the impact of socio-psychological cyber dynamics and highlight the importance of approaches to cybersecurity that emphasise group identity and the importance of mitigating the influence of cyber operations on ethnic, identity, religious and social divides. Mass manipulation of societal identity is a process which marries technical means with socio-psychological dynamics, and this is beginning to be examined and reflected in recent analyses of cyber operations. There is a considerable volume of literature that analyses cyberattacks as a form of coercion or compellence, for example, involving attempts by states to change the behaviour of their adversary through cyber campaigns (Borghard and Lonergan 2017; Buchanan 2014; Hodgson 2018). There has also been an increased focus on the manipulation of social media using personally targeted and emotionally charged news stories and advertising. These can be generated by 'algo-journalism' (journalism driven and produced by algorithms) and may have considerable societal effects, including producing group-emotional behaviour within social networks and the ability to manipulate public sentiment en masse (Bakir and McStay 2018). Such manipulation can create social groups that exist in echo chambers, create 'wrongly informed citizens' and exacerbate the well-established problem of confirmation bias, where individuals and groups search for, and absorb, information that fits their preconceived notions, and induce 'emotional, identity-based political struggle' (162).

While the societal security concept paid some attention to socio-psychological dynamics, it appears to be worth revising the framework in light of the rise of social media, which has the effect of shaping identity, both positively and negatively influencing identity divides, and which has been weaponised to destabilise societies. As we go on to argue in the next section, the convergence of socio-psychological dynamics with cybersecurity concerns became clearly apparent in a series of events in the late 1990s and early 2000s.

Reinterpreting cyberconflict – path dependency, securitisation and the national cybersecurity state

If the societal security approach is an effective theoretical tool to understand recent cyber events, and a potentially more salient policy framework, then how is it that national and military security-based approaches to cybersecurity have become so dominant in the previous two decades? In answering that question, this section analyses several events that led to the emergence and subsequent consolidation of national cybersecurity states and undermined the emergence of a more decentralised, societal approach based on identity conflicts and socio-psychological factors. This is not an extensive history of post-Cold War cyberconflict. Nevertheless, these cases provide snapshots of the process by which cybersecurity was 'securitised' by many governments in the West and national security agencies obtained considerable power in this emergent domain. Cyberattacks were framed in the discourse of political leaders during this period as an existential threat to nations that would cause major disruptions to national economies and be catalysts for

conflict between the great powers. Growing concerns over internet failure and instability and attacks against critical infrastructure were instrumental in creating fear and paranoia, but also served the political and commercial purposes of securitising actors and hindered the emergence of societal approaches. Later in the period, owing partly to the growing influence of social media platforms, the societal effects of disinformation were layered into anxiety-saturated cyber policy. Importantly, these cases also created path-dependencies in which the relationship between government and the societal sector worsened and through which military agencies and structures have taken actions that have intensified societal and cybersecurity dilemmas.

'Millennium madness' – Kosovo and the Y2K bug

The conflict in Kosovo in 1999 was one of the first major conflicts in which cyberattacks were used by warring parties for strategic advantage. In March that year, NATO, while conducting strategic air strikes on the forces of Milosevic, sustained cyberattacks from Serbian hackers targeted at its headquarters and digital infrastructure. In response to the bombing of the Chinese embassy in Belgrade, Chinese hackers also conducted cyberattacks against the White House website, the US departments of energy and the interior and the national parks service, including replacing website content with images and text expressing fury over the bombing. The US military's response exhibited elements of restraint, but Pentagon commanders considered a variety of electronic measures to respond to Serbian hackers and enhance their own operational and political effectiveness through electronic means. This included hacking into Serbian banks to cause economic problems for the regime, trying to isolate Slobodan Milosevic electronically to harm the continuity and centrality of command, and targeting his own personal wealth to bring him to the negotiating table (Borger 1999). The Pentagon's restraint at this time was largely due to legal concerns over whether the use of cyberweapons would constitute war crimes, whether they would be strategically successful, whether they would accelerate the development of offensive cyber tools by foreign power (the security dilemma), and whether the tools used could be reverse engineered or at least reveal US military cyber capabilities and methods (Borger 1999).

The hacks created strong incentives to nationalise and militarise cybersecurity and demonstrated to the US and NATO militaries the seriousness of the cyberthreat they faced. However, the social and psychological elements of the conflict are underappreciated. Kosovo was a typical identity-based conflict, where warring parties were from ethnically aligned, culturally adversarial societal groups. The activities were conducted by non-state hackers, including Serbian and Chinese nationalists, and targeted not only military organisations but the societal sector (parks and energy, for example), illustrating the need for (and lack of) attention to societal cyber vulnerabilities, the spillover effects of military conflicts into the societal sector, and the inability of the US military to respond to hacks and provide assistance to organisations that became entangled in the conflict's electronic dynamics. The hackers involved in hacktivism during the conflict, moreover, were part of global social networks that included traditional anti-war sentiment and groups. It is illustrative of our argument that when NATO intervened in Libya in 2011, 12 years after the war in Kosovo, Serbian hackers conducted similar anti-NATO hacks. In this case, online communities opposed to and influenced by NATO interventions

transcended spatial and temporal boundaries. This was not, however, a lesson prominent in those derived from this and subsequent conflicts. The Kosovo cyberattacks also demonstrated the importance of the informational elements of contemporary conflict and the war of narratives that influences public opinion during conflict situations. The aim of the hackers and the effect of the hacks were to deny and prevent the NATO public affairs website from communicating its narrative around the conflict (the public affairs website was inoperable for several days). In this respect, the tactical and operation effects of the hacking operation, including increasing NATO manpower requirements, slowing operating tempo and enlarging the potential for human error in the air strike operations (Department of Defense 2000) were combined with social and psychological effects targeting perceptions of the conflict among identity groups. Ultimately, none of them caused major damage to the alliance or the US and the impact of these hacks should not be overestimated. In this respect, the acceleration of military capabilities and doctrine that occurred after and because of the conflict may have been disproportionate to the actual threat, which is a common feature of the process of securitisation.

Similar societal and psychosocial dynamics were in evidence as the global community, and particularly the financial sector, faced the prospect of an 'electronic meltdown' caused by the Millennium (Y2K) Bug at the turn of the century. The bug caused widespread fear about the integrity of the global internet and hundreds of billions of dollars were spent by governments around the world to prepare for, and mitigate, potential effects (Jowitt 2017). The bug was a relatively simple glitch in electronic systems caused by the transition from the four-digit date 1999–2000, but nevertheless, caused widespread alarm. In October 1998, President Bill Clinton signed the Year 2000 Information and Readiness Disclosure Act, which was an attempt to encourage private sector (and societal sector) actors to share information about Y2K-related vulnerabilities by offering them limited indemnity against losses or lawsuits resulting from the potential disruption. These attempts to involve the societal sector were not helped, however, by a wider context of securitisation. An issue of Time Magazine was indicative of both the global hysteria and the securitising discourse, raising the prospect of Y2K causing 'The end of the world!?!', citing 'Y2K insanity!', 'Apocalypse Now!', asking 'Will computers melt down? Will society?', providing what it called 'A Guide to Millennium Madness' and citing fears of airlines and banking systems going haywire (Ghishal 2017).

These concerns spilled over into the defence sector, with John Hamre, the US Deputy Secretary of Defense from 1997 to March 2000, contributing to the securitising discourse by arguing that 'the Y2K problem is the electronic equivalent of the El Niño and there will be nasty surprises around the globe' (Jowitt 2017). References by cyber policymakers to extreme weather events, Armageddon, apocalypse, natural disasters, pandemics, biological agents and previous wartime scenarios were commonplace in the early 2000s and such analogies served to structure thinking and as rhetorical tools to add urgency to the securitising process (Betz and Stevens 2013). This rhetoric was accompanied by several more practical measures which set a precedent for military responses to cyber-related incidents. In the UK, for example, armed forces were put on standby to assist in maintaining vital public services in the event of an internet meltdown, including providing disaster relief in the event of hospitals, water supplies and roads and traffic systems being affected (Waugh 1998). In the US, officials noted the possibility of military responses to Y2 K problems and addressed concerns about effects of the bug on nuclear missile

operations (Gershwin 1999). This contributed to a broader process where militaries were searching for new roles in the absence of the Soviet threat and were increasingly planning for involvement in civil crises and emergencies across security sectors. In this way, trends in cybersecurity advanced in parallel with broader securitisation patterns, including in areas such as pandemic response, terrorism and migration.

While the Y2K bug eventually turned out to be a 'damp squib', the fear and uncertainty it generated fed into a new era of collective paranoia which further accelerated the securitisation of the internet and its functions. This included the construction of a perception that the internet lacked resilience and underpinned society in a way that was inherently vulnerable and prone to disintegration (Best 2003). This ran counter to the idea of the internet as a democratising technology, facilitating harmonious relations and technological and societal progress, and exposed 'the fundamental unknowability both of computer technology and of the ultimate value of that technology, its networking capacity, and its generation of information' (Best 2003). As Kasvio (2000) argues, 'Even if the transition to the new Millennium did not cause any major collapses of the existing computer systems, the whole process of preparatory measures showed clearly how strongly the vital functions of modern societies depend on the orderly functioning of extremely complicated systems which nobody fully understands'. The Y2K problem also demonstrated a tendency, which was to become a central feature of cybersecurity debates in the 2000s, to overestimate the risks posed by new technologies, and create disproportionate, centralised and bureaucratic responses. In the words of Quiggin (2005), the Y2K bug created a moral panic in which there was a 'systematic tendency, arising from the nature of the mass media and political processes, to overstate some kinds of threats, particularly those involving new and unfamiliar dangers.' This was compounded by a media that tended to exaggerate the risk, sensationalise stories and not cover government efforts to mitigate risks involved, burdensome as those efforts were (Quigley 2004, 823).

In line with the argument in this article, the Y2K bug also had broader socio-psychological effects and demonstrated the need for governments to manage these (although little was done in the aftermath of any of these events to reconcile these dynamics). These effects are addressed by Kevin Quigley (2004, 825), who argues:

> IT ranks high in the 'dread factor' in psychometric terms; it has the power to unleash considerable anxiety. The more government depends on IT to deliver its service, the more vulnerable it is to a public that oscillates from hyper-reaction to hyper-reaction. Indeed, while IT commentators, both professional and amateur, offer IT as the universal solution to social and organizational problems, Y2 K demonstrates that the 'panacea' can quickly deteriorate to a paradoxical 'organized pandemonium', as in the case of Y2 K. Hence, the government must be sensitive to this potential and must adopt effective communications with key partners, be they suppliers, private industry, the media or civil society at large, to reassure these partners that they are managing IT effectively.

The effectiveness of communication between the government and private sector was not helped during this period by governments' own securitisation of the incident.

9/11 And weapons of mass disruption

The fears generated by the Y2K problem did not subside after the millennium passed but were compounded and intensified in processes that resulted from the 9/11 terrorist

attacks in New York and Washington, DC. The attacks presented a seminal moment in the development of fears around cyberterrorism, especially as enhanced border and aviation security created incentives for non-state actors to try to strike the US remotely through digital networks and digital infrastructure. In the aftermath of the attacks, various measures were taken by the US government to protect the US 'homeland', and these extended into cyberspace. Concrete examples of enhanced digital security measures included the Patriot Act, which allowed the US government unprecedented powers to access electronic communications, and the now widely-covered activities of the US National Security Agency, including the Prism programme, which enabled the agency to identify and target illegal and extremist activity online through 'mass surveillance'. The war on terror served to further nationalise security in the US, created powerful new bureaucracies, including the Department for Homeland Security, which was given strong statutory authority to respond to cyberthreats. The empowerment of the intelligence community was also a feature of the post 9/11 environment and a variety of agencies took on a role in online operations against terrorists and rogue states. This powerful national cybersecurity state was not best aligned to match the challenge of globally connected systems of computers and the debates that emerged within the national security community over deterrence and pre-emption returned to Cold War concepts. There was a tendency, for example, to equate weapons of mass disruption (cyberweapons) with weapons of mass destruction and a close association emerged between digital threats and physical – and even nuclear – threats to American and its allies in the aftermath of 9/11. Former Defense Secretary Leon Panetta's warning of a 'cyber pearl harbour' (Bumiller and Shanker 2012) is perhaps the most famous and widely cited example, but there were many others. These warnings appear to have been unrealistic and fears around terrorism and the capability of non-state actors to mount large scale and sophisticated cyberattacks have largely proved unfounded.

The most fundamental problem here was a failure to identify that 'cyberterrorism' – cyberattacks causing equivalent effects to conventional terrorist attacks – was not such a serious threat as feared and constructed by national security agencies. In this sense, cyberterrorism was based on fears that were not accurately assessed and which fuelled securitisation processes. A secondary problem was the widespread conflation between cyberterrorism (a very limited problem by any measure) and terrorist use of the internet (a more serious and pervasive issue). The 'cyber 9/11' scenario failed to materialise for various reasons, including the fact that cyberattacks do not create the powerful visual effects that more conventional acts of terrorism do; that the difficulty of attributing cyberattacks does not allow terrorist groups to derive the propaganda benefit of being held clearly responsible for such attacks; and the lack of scientific and technical expertise to pull off more than just nuisance type acts of cybervandalism. Despite these now seemingly obvious dynamics, the term cyberterrorism entered the national security discourse and often went unchallenged. As Sean Lawson (2013, 86) has argued, 'cyber-doom scenarios are the latest manifestation of fears about 'technology-out-of-control' in Western societies,' and are 'unrealistic' and 'encourage the adoption of counterproductive, even dangerous policies.' In this context it is worth noting that, in some cases, states have taken military actions against hackers associated with terrorist groups, including the targeted killing by US forces of an ISIS hacker in 2016 and the more recent Israeli military attack against a Hamas cyber facility. These kinetic responses do not appear to have

been based on the likelihood of physical damage being caused by cyber operations, but in response to hack and leak operations in the US case (the ISIS hacker has released hacked details of US military personnel), and a Hamas cyber operation which had already been fended off by Israeli cyber defences (Newman 2019). In this respect, and in line with the arguments of this article, terrorism presents an arguably greater societal threat than it does to the military, stems from identity divides that terrorist groups prey on and exploit and has led to over-militarised responses which have fed existing identity-based conflicts.

WannaCry – the result of cyber path dependency

If 9/11, the Millennium Bug and Kosovo created path dependencies in cybersecurity, where did that pathway lead? The pitfalls and consequences of taking an overly national security-led approach to the issue of cyberthreats were certainly in evidence with the global spread of the WannaCry ransomware in 2017 and there are several reasons why this case demonstrates the analytical relevance of the societal security approach and furthers the arguments around securitisation highlighted above.

First, the scope of the attack was unprecedented in the impact it had on society. It was the most widespread ransomware virus hitherto deployed, affecting hundreds of thousands of computers in 150 countries, (Strategic Comments 2017) and caused widespread fear and anxiety. While the 'ransom' generated from the attack was relatively low – approximately $150,000 USD (Twitter 2020) – the damages caused have been estimated at around $4 billion USD (Berr 2017). The ability of the purveyors of the ransomware to seize computers from their owners on a global scale had not been as evident up until this point. The wider societal impact of the attacks were also striking, especially in the way they bypassed the traditional security structures that were designed to enhance national security. This is perhaps best articulated in Christensen and Liebetrau's analysis of WannaCry (2019), in which they argue that cybersecurity 'evades the state as the natural political fulcrum of security politics'. Some of the most prominent effects were noted in the healthcare system in the UK, the NHS, where operating systems running Windows XP were particularly vulnerable. Many other societal actors were affected, including services, manufacturing, public administration, finance and trade (Loesche 2017).

Second, the WannaCry case illustrated how harmful national security practices could spill into the societal realm. The WannaCry ransomware was based on the EternalBlue exploit, a Windows XP vulnerability, that the NSA had known about but not disclosed. This is illustrative of a broader tendency to overclassify cyberthreats and indeed to stockpile them for espionage and offensive cyber operations. These dynamics were further illustrated by the messy geopolitics surrounding the incident, with the US and UK governments attributing the attack to the North Korean regime, the leak of the exploit purportedly resulting from the activities of the 'Shadow Brokers' hacking group, themselves linked to Russian state intelligence, and further speculation by Edward Snowden that the leak was a response to US public attribution of malicious cyber activity conducted by Russian authorities. However the event is attributed, and whoever was responsible for the leak and the deployment of the ransomware itself, the case clearly demonstrates the perils of the development of offensive cyber capabilities in the national defence and

intelligence communities and a lack of communication between these agencies and the private sector. If the NSA had disclosed the vulnerability to Microsoft, patches could have been released.

It should also be noted that the 'kill switch' which disabled the ransomware was not found by the security agencies, but by a malware analysis expert, MalwareTech (who was incidentally later charged for a separate case of hacking) – demonstrating both the need for bottom-up, people-centred responses to these types of events and that national security agencies will not always have the skills or capabilities to stop major cyberattacks. While WannaCry is clearly not the end point of post-Cold War cyberconflict, the path dependencies created around the Millennium certainly appear to have ended up with a narrow form of national self-interest prevailing over patching vulnerabilities, a lack of corporate responsibility around cyberthreats (Microsoft were not releasing patches for Window XP, for reason of cost rather than security), the overclassification and centralisation of vulnerabilities, the broader tendency for national security agencies to not disclose information and not to be transparent about offensive cyber capabilities (Greenberg 2017), and a lack of attention to the societal impact of major cyber breaches. The aforementioned issues around market consolidation and other economic factors were also at play here, with the attack spreading far and fast because of the global dominance of the Windows operating system and the lack of investment in societal sector digital infrastructure, which was an important contributing variable in the damage caused.

Desecuritisation and cybersecurity

The Kosovo War, the Millennium Bug, and the war on terror acted as catalysts for the emergence of a form of cyber securitisation at a crucial early period in post-Cold War history and demonstrated both how cyberconflict could spill over into the physical realm and geopolitics could spill into the cyber realm. They also provided the political context and ordering ideas and concepts that fed into the emergence of social media networks in the mid-2000s and the recent growth of system-wide cyberattacks, such as Wannacry. But while much of the academic literature on securitisation describes the process by which issues become securitised, the reverse process, where issues are desecuritised, is undertheorized (Coskun 2008) and has not yet been substantively applied to cybersecurity debates and issues. Articulated most clearly by Buzan and Wæver (2003, 489), desecuritisation is 'a process in which a political community downgrades or ceases to treat something as an existential threat to a valued referent object and reduces or stops calling for exceptional measures to deal with the threat'. But how can this be achieved and what are the potential obstacles and barriers to cyber desecuritisation more specifically?

If securitisation is a process driven by ontological insecurity, defined here as an erosion of identity and an anxiety created and fuelled by globalisation, then the place to start in a process of cyber-desecuritisation must be to reframe discourse and present cyber 'threats' in less apocalyptic, fearful tones. This involves moving towards a normalised and less polemic political debate in which cybersecurity is not continually treated as an emergency but rather as a regular feature of modern political interactions. It also means avoiding the Cold War, WW2, and biological analogies that have dominated cybersecurity discourse. Changing cyber metaphors in this way could lead to better cyber policy and placing

emphasis on more positive environmental language, such as 'healthy ecosystems', might generate wider discursive progress (Lawson 2012). In other words, if securitisation involves framing an issue as an existential threat, a process of desecuritisation must do the opposite – highlight the real impact and not the expected or likely impact – to ease tensions and fear created by cyberattacks, and to manage threats rather than overreact to them. This will necessarily involve recognising that cyberattacks exacerbate identity divides and working consciously to move past characterisations of cyberattacks as technical tools of state conflict, portraying them instead as extensions of historical, cultural and political disputes within and between states and societal groups. Cyberattacks may have serious consequences, but pose less threat than natural disasters, climate change, nuclear weapons, and biological agents and pandemics. This observation has come into stark relief in the context of COVID 19, which has caused over a million deaths, as opposed to cyberattacks, which, as a result of a recent attack against a hospital in Germany, appear to have now caused just one (Wetsman 2020). As this article has shown, however, the fear they create drives responses that are out of sync with the level of threat involved.

The Copenhagen School itself recognised the utility of these options, describing three core processes that desecuritisation can be based upon. The first is to not talk about issues in terms of security in the first place (Wæver 2000). Cleary, the rhetoric that cyberattacks have created over the last two decades render this option obsolete. However, changing the language *from now on*, being more cautious about presenting cyberattacks as an existential threat, and toning down the cyber rhetoric could help the process of desecuritisation. Specific policy commitments could be made by governments not to further securitise cyber, to construct common language across domestic and international political entities that does not fuel securitisation processes and, considering the influence of commercial and media entities in the cases described above, to encourage responsible reporting and advertising that does not create fear either to sell newspapers or cybersecurity products.

The second option when an issue has already been securitised, as in the case of cybersecurity, is to avoid creating security dilemmas (societal and interstate). Securitisation in cyberspace has involved the implementation of defensive measures to protect computer networks. These include technical, human and virtual tools. But defensive actions can be interpreted as offensive ones. This is the nature of the security dilemma. The blurring of the distinction between cyberattack and defence, and the creation of modes of 'active cyber defence' and pre-emptive network intrusions, has furthered the mistrust and misperception that exist between prominent cybersecurity actors. In the most substantive analysis of security dilemmas in cyberspace, Ben Buchanan (2016) argues that intelligence collection, or cyberespionage, creates and exacerbates cybersecurity dilemmas, especially as there is a strong link between intelligence collection and network attack. It is unreasonable to suggest that intelligence agencies are going to stop intruding on adversary networks – this pattern of activity seems to be widely accepted and commonplace in the contemporary era. However, progress has been made in limiting the activities of intelligence agencies and prosecuting foreign adversary hackers when involved in commercial cyberespionage, and there has been some attempt to reach agreements between the leading powers to limit the scope of commercial cyberespionage, as in the case of the agreement between Xi Jinping and President Obama in 2016. Avoiding security dilemmas

will also involve ongoing dialogue and negotiation between the states even within a context of 'cheating' – measures taken to circumvent existing agreements, which is what has occurred since the agreement between the US and China, with a notable increase in Chinese espionage observed during the Trump administration (Harold, Libicki, and Cevallos 2016). Buchanan further argues that mitigating the cybersecurity dilemma involves building baseline defences (these will be particularly important in the societal sector), building trust between adversaries (difficult in the existing deteriorating environment, but not impossible), taking unilateral steps to increase international stability (including, for example, reporting zero-day vulnerabilities, and establishing and communicating a posture for dealing with the intrusions when they inevitable do occur). These steps, when combined with a discursive commitment to lower the cyber rhetoric and hyperbole, may constitute significant progress towards desecuritisation.

A third option to desecuritise involves efforts to move security issues back into normal politics. There are already some efforts underway to do this. The emergence of the cyber resilience concept is one such reformulation which recognises that total security of computer networks is unachievable, that breaches will occur, and that the ability of systems to recover and be quickly replaced provides a more realistic aim and goal. Resilience in the societal sector acts both as a less polemic rhetorical tool and an opportunity to shift responsibility for cybersecurity away from the national security state, a process which has been underway in multiple world regions, including in the EU area and in Asia, since at least 2012. It should be noted, however, that that the resilience concept is not a panacea for cyber desecuritisation and has been criticised as being part of securitisation processes themselves (an excuse to give governments an intrusive role in the societal sector) (Bourbeau and Vuori 2015) and a product of contemporary neoliberalism (Bourbeau and Ryan 2017).

The question that remains largely unanswered, and which may resolve some of the tensions between state and society, is: who is responsible for desecuritisation? Changing the discourse from security to resilience is one such rhetorical example which has policy implications, but there will also need to be a process whereby desecuritising actors counter the securitising actors that have driven cyberthreat rhetoric in recent years. These actors could be the same, such as the military officials, government and policy circles, the media and the military itself. In this way, the securitising actors will drive desecuritisation. As Aradau (2004) argues, however, this may be both undesirable and difficult. There are powerful political interests that have a stake in securitisation processes and there has been a tendency for both commercial and political entities to hype the cyberthreat because it sells cybersecurity products and tools and creates incentives to drive policy and the development of new national security capabilities and functions. In the military realm, and particularly in the intelligence apparatus of many states, cyberthreats create avenues to enhance bureaucratic and political influence. In this sense, depoliticising threats is a necessary component of desecuritisation and the desecuritising actors should not be those responsible for securitising processes (Aradau 2004).

This naturally shifts the emphasis for desecuritisation efforts towards the role of the societal sector, whose role in the event of cyber incidents that cause widespread disruption or damage, or that cause political/social effects, needs to be considered more fully. If responsibility for cybersecurity is to be shifted away from military and intelligence agencies, then the societal sector must step forward. But who and what are we talking

about here? Without getting into a much deeper philosophical debate about what society is, the tendency so far has been to view societal actors in cybersecurity through the lens of critical infrastructure protection (CIP) – defined by the Department of Homeland Security as consisting of 16 key sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams Sector; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Waste; Transportation Systems; Water and Wastewater Systems Sector (Department of Homeland Security 2013). But while these constitute areas of areas of activity on which society depends, a further shift is required to conceptualise societal actors more broadly and to recognise that while these sectors are important to the functioning of society, they are not as critical to its cohesiveness. In this respect, and as appears to be already happening, a wider conception of 'critical infrastructure' may be needed, as well as a wider conception of societal actors that shifts the debate towards socio-psychological and identity-based concerns. This should include online and physical social networks and movements, local government, democratic processes and governance, attacks against vulnerable groups (the elderly have suffered through the wave of COVID 19-related cybercrime, for example), the education sector (schools and universities) and ethnic, religious, gender and other identity groups, who often experience the effects of cyber operations disproportionately. This would mean the state not just recognising the importance of securing the critical infrastructure on which society depends, but also making a shift securing society *itself* from cyber operations.

Other desecuritising actors could include civilian agencies of government. The police, for example, have not shown a tendency to securitise cyberthreats to the extent that national militaries and intelligence agencies have, and they could play a greater national and international role in cyber defence. In this context, cybersecurity and cyberwarfare are often conflated with cybercrime and making more accurate distinctions between them will help to accelerate desecuritising moves. More responsibility could be also given to civil society too, both within states, and in international fora, a variety of which do provide at least some avenues for discussion between states that are often on opposite sides of the cyberwarfare divide. This might include the Open-Ended Working Group at the UN, ICANN, and/or the Organisation for Security and Cooperation in Europe (OSCE) pursuing a cyber desecuritisation agenda and reflecting desecuritising practices in their policies, dialogues and frameworks. The technology sector will be important here too. If cyber is to be desecuritised, then the major social media platforms and software and hardware providers clearly need to play a role, including in changing the discourse around cyberthreats and resisting efforts by the national security community to instrumentalise their technologies for military-strategic purposes.

At least initially, and because of the ongoing importance of the state, such moves towards desecuritisation will likely involve the national security sector working more consistently with societal actors (and the tech companies themselves). There is some evidence of this already happening, including cyber resilience reviews conducted by the US Department of Homeland Security, for example. But progress needs to occur in other core areas. The first is information sharing within and between societal sectors on cyberthreats. New institutional mechanisms need to be in place to address this issue and forms of societal sector confidence building and trust building need to be

established. This is especially true in the context of a major cyberattack that has a wide societal impact. The finance, energy, transport, telecommunications, social media, and democratic governance sectors need to have ways to communicate and share information on attack vectors, methods, and patches and remedies. These could be facilitated by, but should not be dependent upon, national security apparatus. To be more specific to policy, new mechanisms are needed for information sharing on cyberthreats in these sectors, and national cyber authorities should integrate them into their incident response procedures and structures.

The second area that needs to be developed is service continuity in the societal sector. Much work needs to be done to develop and exercise specific plans to maintain digital and societal services in the event of major internet outages. In the democratic governance sector, this might involve having paper ballot systems to back up electoral processes that rely on machines and digital networks; in the energy sector, plans to fill the gap in supply caused by internet outages; and in the transport sector, contingency plans to deliver products and services. As a Research Council of Norway report (2014) notes, 'The point of departure for societal security efforts is that crises can and must be prevented. This implies understanding their causes and preventing threats or hazards from manifesting themselves. If crises nonetheless arise, they must be dealt with in the best possible manner.' Sectors should not be isolated, however, and the spillover effects across sectors should be addressed. As Kirsten Neilsin, the former US Homeland Security chief recently recognised, 'We cannot get stuck in silos and focus on vulnerabilities in specific sectors,', cyberattacks have 'untold cascading consequences' (Lillington 2018). That some of the theoretical premises of the societal security approach are beginning to be reflected by policymakers is encouraging, but more clearly needs to be done, including involving the civil sector as opposed to the military in emergency/crisis response measures. Societal actors (including private companies and civil society) could also do more to attribute cyberattacks, especially as, at least in some observed cases, they can act faster and have fewer concerns about disclosing attribution methods (Eichensehr 2019).

Conclusion

We have presented the argument that a shift needs to occur in cybersecurity theory and policy. One way of achieving this is through the application of the societal security approach and its adaption and application to cyberthreats. The approach has been applied to other policy areas with considerable benefit to our understanding of contemporary security issues and in finding ways to actively address them. To shift responsibility to the societal sector, a process of de-securitisation is necessary. This involves framing cyberthreats differently, both through general discourse, but also consciously, through policy formulation and in the media. We recognise that this process will be confronted by powerful political, bureaucratic and commercial interests.

In making this argument, we do not propose that military cyberthreats should not be taken seriously, or that the military and intelligence agencies should not have a role in cybersecurity. Buzan's conceptualisation of security recognised that the military had an ongoing role. The arguments that cyberattacks can be used for force protection and/or in place of the use of military force have merit. What we *are* arguing for is that the military

and intelligence community 'stay in lane', recognise the spillover effects of strategic cyberconflict, and are not the lead players in societal security efforts, but play a coordinating role. There are two other potential perils in this approach – the first is that society itself is not coordinated enough to address societal threats effectively. This is rooted in one of the core critiques of societal security as a theory, which is that there has been a tendency to reify societies as independent social agents (Theiler 2003). As others have argued, there has been a reluctance in the private (and indeed societal) sector to take on responsibility or liability for cybersecurity (Carr 2016), especially where it would entail considerable costs and a reluctance by governments to pass on responsibility for security to the private sector (Dunn Cavelty and Brunner 2007). There are very strong headwinds here, including a continued predisposition to use securitising discourse, the ongoing power of the national security state, a deteriorating global geopolitical environment, and the continued dominance of big tech. Nevertheless, it is a fundamental requirement for a more effective, less conflictual cybersecurity environment to emerge. Second, the role that society takes in cybersecurity should not lead to the same practices that intelligence agencies and military institutions have been engaged in, including surveillance, intrusions into privacy and the creation of fear and mistrust within and between communities. In other words, moving towards a societal cybersecurity approach should not entail securitising society itself. This concern has been addressed in some detail through the Foucauldian school of securitisation theory (see Schuilenburg 2012) and highlights that avoiding negative consequences will involve effective multi-stakeholder management of cyber issues at the local level.

The theoretical implications of this article are worth closing with. A continued predisposition to view cybersecurity as an issue of national security exists in the literature. Theoretical frameworks that rely on identity, discourse and societal dynamics are still underdeveloped and underapplied to cybersecurity issues. Continuing to adapt and supplement these frameworks with societal and socio-psychological analyses of the causes and impact of cyberattacks is, in our view, one of the most important research agendas in the still emerging cybersecurity discipline. We contend that the historical evidence presented in this article has highlighted the lack of attention to these issues and their general validity in understanding how the cybersecurity environment has evolved.

Acknowledgments

The authors would like to convey our sincere thanks to the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) for supporting this project when it was in an early stage of development. Clare Lain worked at the centre and Joe Burton was a visiting researcher there during this period.

We would also like to thank the two anonymous reviewers and the editors for their constructive and helpful comments.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

Research for this article received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 844129.

Notes on contributors

Joe Burton is a Marie Curie Fellow at Université libre de Bruxelles, completing the two-year European Commission-funded project Strategic Cultures of Cyber Warfare (CYBERCULT). He is also a senior lecturer in the New Zealand Institute for Security and Crime Science, University of Waikato. He holds a Doctorate in International Relations and a Master of International Studies degree from the University of Otago and an undergraduate degree in International Relations from Aberystwyth University. He is a recipient of the US Department of State SUSI Fellowship, the Taiwan Fellowship, and has been a visiting researcher at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Joe is the author of *NATO's Durability in a Post-Cold War World* (SUNY Press, 2018), editor of *Emerging Technologies and International Security: Machines, the State and War* (Routledge, 2020), and his work has been published in *Asian Security*, *Defence Studies*, *Political Science* and other leading academic publishers.

Clare Lain joined the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in January 2016 as the UK Senior National Representative and was there for four years. As part of the Strategy Branch, she had responsibility for delivery of the NATO doctrine for Cyberspace Operations and the creation and delivery of a bi-annual Seminar for Senior Executives from both civilian and military organisations. Other areas of research and specialism include the role of cyber in a hybrid scenario and response, in particular its relationship to electronic warfare; the influence of cyber in other disciplines such as intelligence, the Estonian Start-Up community and the Military Police; and the role of society in a major cyber incident. Clare now works at the UK Hydrographic Office where she manages relationships with international bodies and other member states in regard to the creation and governance of the technical standards for hydrography. She is also responsible for the UKHO's strategy for, and implementation of, new and evolving standards.

References

Agrafiotis, I., J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton. 2018. "A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate." *Journal of Cybersecurity* 4 (1): 1–15.

Aradau, C. 2004. "Security and the Democratic Scene: Desecuritization and Emancipation." *Journal of International Relations and Development* 7 (4): 388–413.

Bakir, V., and A. McStay. 2018. "Fake News and The Economy of Emotions." *Digital Journalism* 6 (2): 154–175.

Berr, J. 2017. "'WannaCry' Ransomware Attack Losses could reach $4 Billion." *CBS News*, May 16. Accessed 1 October 2020. https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

Best, K. 2003. "Revisiting the Y2K Bug: Language Wars Over Networking the Global Order." *Television & New Media* 4 (3): 297–319.

Betz, D. J., and T. Stevens. 2013. "Analogical Reasoning and Cyber Security." *Security Dialogue* 44 (2): 147–164. doi:10.1177/0967010613478323.

Bilgin, P. 2003. "Individual and Societal Dimensions of Security." *International Studies Review* 5 (2): 203–222.

Black, S. 2012. "The Blowback and Collateral Damage of Cyber-warfare." *Business Insider*, June 13. Accessed 6 September 2020. https://www.businessinsider.com/the-blowback-and-collateral-damage-of-cyber-warfare-2012-6?IR=T.

Bloomfield, A. 2012. "Time to Move On: Reconceptualizing the Strategic Culture Debate." *Contemporary Security Policy* 33 (3): 437–461. doi:10.1080/13523260.2012.727679.

Borger, J. 1999. "Pentagon Kept the Lid on Cyberwar in Kosovo." *The Guardian*, November 9. Accessed 20 May 2020. https://www.theguardian.com/world/1999/nov/09/balkans.
Borghard, E. D., and S. W. Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26 (3): 452–481.
Bourbeau, Philippe, and Caitlin Ryan. 2017. "Resilience, Resistance, Infrapolitics and Enmeshment." *European Journal of International Relations* 24 (1): 221–239.
Bourbeau, Philippe, and Juha A. Vuori. 2015. "Security, Resilience and Desecuritization: Multidirectional Moves and Dynamics." *Critical Studies on Security* 3 (3): 253–268.
Branch, J. 2020. "What's in a Name? Metaphors and Cybersecurity." *International Organization*, 1-32. doi:10.1017/S002081832000051X
Brantly, A. 2016. *The Decision to Attack: Military and Intelligence Cyber Decision-Making*. Athens: University of Georgia Press.
Buchanan, B. 2014. "Cyber Deterrence Isn't MAD; It's Mosaic." *Georgetown Journal of International Affairs* 15 (2): 130–140.
Buchanan, B. 2016. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. London: Hurst.
Bumiller, E., and T. Shanker. 2012. "Panetta Warns of Dire Threat of Cyberattack on U.S." *New York Times*, October 11. Accessed 20 May 2020. https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.
Buzan, B. 1997. "Rethinking Security after the Cold War." *Cooperation and Conflict* 32 (1): 5–28.
Buzan, B. 2007. *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. Colchester: ECPR Press.
Buzan, B., and O. Wæver. 2003. *Regions and Powers: The Structure of International Security*. Cambridge: Cambridge University Press.
Carr, J. 2010. "Did the Stuxnet Worm Kill India's INSAT-4B Satellite?" *The Firewall*, September 29. Accessed May 20 2020. https://www.forbes.com/sites/firewall/2010/09/29/did-the-stuxnet-worm-kill-indias-insat-4b-satellite/#22772825127d.
Carr, M. 2016. "Public-Private Partnerships in National Cyber Security Strategies." *International Affairs* 92 (1): 43–62.
Christensen, K. K., and T. Liebetrau. 2019. "A New Role for 'The Public'? Exploring Cyber Security Controversies in the Case of WannaCry." *Intelligence and National Security* 34 (3): 395–408. doi:10.1080/02684527.2019.1553704.
Coskun, B. B. 2008. "Analysing Desecuritisations: Prospects and Problems for Israeli–Palestinian Reconciliation." *Global Change, Peace & Security* 20 (3): 393–408. doi:10.1080/14781150802394337.
Demchak, C. C., and P. Dombrowski. 2011. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5 (1): 32–61.
Denning, D. E. 2011. "Cyber Conflict as an Emergent Social Phenomenon." In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by T. Holt, and B. Schell, 170–186. Hershey, PA: IGI Global.
Department of Defense. 2000. "Kosovo/Operation Allied Force After Action Report." Report to Congress, January 31.
Department of Homeland Security. 2013. "National Infrastructure Protection Plan." Accessed 1 October 2020. https://www.cisa.gov/national-infrastructure-protection-plan.
Dunn Cavelty, M., and E. M. Brunner. 2007. "Introduction: Information, Power, and Security—an Outline of Debates and Implications." In *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*, edited by Myriam Dunn Cavelty, Victor Mauer, and Sai Felicia Krishna-Hensel, 1–18. Aldershot: Ashgate.
Eichensehr, K. 2019. "Cyberattack Attribution and the Virtues of Decentralization." *Just Security*, July 3. Accessed 20 May 2020. https://www.justsecurity.org/64755/cyberattack-attribution-and-the-virtues-of-decentralization/.
Geer, D., E. Jardine, and E. Leverett. 2020. "On Market Concentration and Cybersecurity Risk." *Journal of Cyber Policy* 5 (1): 9–29.

Gershwin, L. K. 1999. "Foreign Preparedness for Y2K Statement for the Record House International Relations Committee." *CIA*, October 21. Accessed 20 May 2020. https://www.cia.gov/news-information/speeches-testimony/1999/gershwin_testimony_102199.html.

Ghishal, A. 2017. "US Government will Stop Battling the Y2K Bug at Last." The Next Web, June 16. Accessed 20 May 2020. https://thenextweb.com/us/2017/06/16/us-government-will-stop-battling-the-y2k-bug-at-last/.

Gioe, D. V., M. S. Goodman, and A. Wanless. 2019. "Rebalancing Cybersecurity Imperatives: Patching the Social Layer." *Journal of Cyber Policy* 4 (1): 117–137.

Glisinan, K. 2018. "If Terrorists Launch a Major Cyberattack, We Won't See It Coming." *The Atlantic*, November 1. Accessed 20 May 2020. https://www.theatlantic.com/international/archive/2018/11/terrorist-cyberattack-midterm-elections/574504/.

Gomez, M. A., and E. B. Villar. 2018. "Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats." *Politics and Governance* 6 (2): 61–72.

Greenberg, A. 2017. "Hold North Korea Accountable for WannaCry – and the NSA, Too." *Wired*, December 19. Accessed 1 October. https://www.wired.com/story/korea-accountable-wannacry-nsa-eternal-blue/.

Guadagno, R. E., R. B. Cialdini, and G. Evron. 2010. "What About Estonia? A Social Psychological Analysis of the First Internet War." *Cyberpsychology, Behavior, and Social Networking* 13 (4): 447–453.

Hang, R. 2014. "Freedom for Authoritarianism: Patriotic Hackers and Chinese Nationalism." *Yale Review of International Studies*, October. Accessed 20 May 2020. http://yris.yira.org/essays/1447.

Hansen, L., and H. Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53 (4): 1155–1175.

Harold, S. W., M. C. Libicki, and A. S. Cevallos. 2016. *Getting To Yes With China in Cyberspace*. Santa Monica, CA: RAND Corporation. Accessed 20 May 2020. https://www.rand.org/pubs/research_reports/RR1335.html.

Hodgson, Q. 2018. "Understanding and Countering Cyber Coercion." In *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*, edited by T. Minárik, R. Jakschis, and L. Lindström, 73–88. Tallinn: NATO CCDCOE Publications.

Janofsky, A. 2018. "Overclassification of Cyber Threats Puts Businesses at Risk." *The Wall Street Journal*, October 31. Accessed 20 May 2020. https://www.wsj.com/articles/gen-michael-hayden-overclassification-of-cyber-threats-puts-businesses-at-risk-1541018014.

Jowitt, T. 2017. "Tales In Tech History: The Y2K Bug." *Silicon*, May 12. Accessed 20 May 2020. https://www.silicon.co.uk/security/firewall/tales-tech-history-y2k-bug-211625.

Kasvio, A. 2000. "Towards a Wireless Information Society: The Case of Finland." Paper presented at lecture series at University of Tampere, Finland, autumn 2000. Accessed 20 May 2020. http://www.info.uta.fi/winsoc/engl/lect/progr.html.

Lawson, S. 2012. "Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States." *First Monday*. Accessed 11 July 2019. https://firstmonday.org/ojs/index.php/fm/article/view/3848/3270.

Lawson, S. 2013. "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics* 10 (1): 86–103.

Lillington, K. 2018. "Cybersecurity 'Everyone's Problem' across Society – US Security Chief." *The Irish Times*, April, 17. Accessed 20 May 2020. https://www.irishtimes.com/business/technology/cybersecurity-everyone-s-problem-across-society-us-security-chief-1.3465066.

Loesche, D. 2017. "Ransomware: Who's Affected & Why." *Statista*, May 15. Accessed 20 May 2020. https://www.statista.com/chart/9378/distribution-of-global-ransomware-infections-and-leading-causes/.

McDermott, D. 2019. "Some Emotional Considerations in Cyber Conflict." *Journal of Cyber Policy* 4 (3): 309–325.

Muncaster, P. 2012. "Patriotic Hackers face off in South China Sea." *The Register*, April 27. Accessed 26 September 2020. https://www.theregister.com/2012/04/27/philippine_china_hack_stand_off/.

Newman, H. L. 2019. "What Israel's Strike on Hamas Hackers Means For Cyberwar." *Wired*, June 5. Accessed 9 December 2020. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

Oskui, R. 2018. "The 5 Industries Most Vulnerable to Cyber-Attacks." *CDNetworks*, December 11. Accessed 20 May 2020. https://www.cdnetworks.com/cloud-security/the-5-industries-most-vulnerable-to-cyber-attacks/.

Quiggin, J. 2005. "The Y2K Scare: Causes, Costs and Cures." *Australian Journal of Public Administration* 64 (3): 46–55.

Quigley, K. 2004. "The Emperor's New Computers: Y2K (Re)Visited." *Public Administration* 82 (4): 801–829.

Research Council of Norway. 2014. "Research for a Safer Society, Research Programme on Societal Security and Risk – SAMRISK." http://ec.europa.eu/DocsRoom/documents/946/attachments/1/translations/en/renditions/pdf, Accessed 20 May 2020.

Rid, T. 2012. "Think Again: Cyberwar." *Foreign Policy* 192 (March 2012): 81.

Roe, P. 2004. *Ethnic Violence and the Societal Security Dilemma*. Florence: Routledge.

Schuilenburg, M. 2012. "The Securitization of Society: On The Rise of Quasi-Criminal Law and Selective Exclusion." *Social Justice* 38 (1/2): 73–89.

Slayton, R. 2017. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41 (3): 72–109.

Stevens, T. 2012. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy* 33 (1): 148–170.

Strategic Comments. 2017. "The WannaCry Ransomware Attack." *International Institute for Strategic Studies* 23 (4): 7–9.

Theiler, T. 2003. "Societal Security and Social Psychology." *Review of International Studies* 29 (2): 249–268.

Twitter. 2020. "Actual Ransom." Accessed 1 October. https://twitter.com/actual_ransom.

Valeriano, B., and B. Jensen. 2019. "The Myth of the Cyber Offense: The Case for Restraint." *CATO Institute*, January 15. Accessed 2 March 2020. https://www.cato.org/publications/policy-analysis/myth-cyber-offense-case-restraint.

Wæver, O. 2000. "The EU as a Security Actor: Reflections from a Pessimistic Constructivist on Post Sovereign Security Orders." In *International Relations Theory and the Politics of European Integration*, edited by M. Kelstrup, and M. C. Williams, 250–294. New York: Routledge.

Waugh, P. 1998. "Army on Call for Year 2000 'Bug' Trouble." *The Independent*, September 11. Accessed 20 May 2020. https://www.independent.co.uk/news/army-on-call-for-year-2000-bug-trouble-1197312.html.

Wetsman, N. 2020. "Woman Dies during a Ransomware attack on a German hospital." *The Verge*, September 17. Accessed 26 September 2020. https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity.