CIVIL DEFENCE GAPS

UNDER CYBER BLITZKRIEG

Discussion Paper

For the International Conference, "Research and Education for the Cyber Storm"
18 January 2019

UNSW Canberra

Greg Austin

ABSTRACT

The paper sets out some background on the concept of *cyber storm* since the weather metaphor was given some currency beginning in 2006. Looking to the future, the paper then suggests that *cyber blitzkrieg* may be a more appropriate term, since states are contemplating sustained multi-vector, multi wave information attacks in which suddenness (including pre-emption) may be an essential characteristic. The paper then gives an overview of the concept of civil defence, including the idea that a civil defence gap can affect strategic military deterrence in certain circumstances. The paper reviews in brief the evolution of cyber civil defence in the two decades beginning in 1998, suggesting that by 2016 the major powers had identified a new urgency that speaks more to the fear of cyber blitzkrieg than to fear of a cyber storm. In the United States, in May 2017, after a decade of incremental policy reform that was increasingly judged to be inadequate, President Trump issued an Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure that demanded a new paradigm of understanding and action. The paper then provides some highlights from the academic literature that pertain to the subject of this turning point, building off a review published in 2016 of the research on dependencies in cyber space. That review confirmed a very low level of global engagement, outside of several U.S. based-research centres, in the policy dynamics of cyber civil defence for extreme contingencies. On that basis, the paper suggests nineteen civil defence "mini-gaps"; and puts forward ideas on what good cyber civil defence might therefore look like to address these. The paper concludes that all states, including the most powerful, are facing a contested, catch-up challenge in cyber civil defence in which paradigm-changing decisions about priorities, reform strategies, budgets and international alliances seem inescapable.

Contents

LIST OF ACRONYMS

AEMO	Australian Electricity Market Operator
APTs	Advanced Persistent Threats
ASEAN	Association of Southeast Asian Nations
BIS	Bank of International Settlements
BRICS	Brazil, Russia, India, China, South Africa (group)
CFDI	Critical Foreign Dependencies Initiative
CIA	Central Intelligence Agency
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIKT	Critical Infrastructure and Key Systems
CMU	Carnegie Mellon University
CRR	Cyber Resilience Review
DARPA	Defense Advanced Projects Research Agency
DHS	Department of Homeland Security
DoD	Department of Defense (United States)
GCSC	Global Commission on Stability in Cyberspace
GGE	Group of Governmental Experts
ICDO	International Civil Defence Organisation
ICRC	International Committee of the Red Cross
ICT	Information and communications technology
INL	Idaho National Laboratory
IOSCO	International Organisation of Securities Commissions
JCS	Joint Chiefs of Staff (United States)
NASCIO	National Association of State Chief Information Officers (United States)
NATO	North Atlantic Treaty Organisation
NCCIC	National Cybersecurity and Communications Integration Center (United States)
NIAC	National Infrastructure Advisory Council (United States)
OECD	Organisation for Economic Cooperation and Development
OSCE	Organisation for Security and Cooperation in Europe
R&D	Research and Development
WFE	World Federation of Exchanges

DRAFT 18 JAN 2019

Introduction

Governments in the wealthiest countries have individually committed hundreds of billions of dollars to buy the most advanced weapons platforms for the contingency of major war between 2030 and 2060. Few of those governments have yet to imagine, let alone budget for, the civil defence force that will be needed in such a contingency to protect national resilience in cyberspace, both for sustaining their military operations and for protecting their civilians. A major war in 2030 would be dominated by mass information operations, including both classic influence operations and cyber sabotage. As the decades wear on, such a war would increasingly be characterised by autonomous weapons systems, and military robots, all dependent on advanced information technologies that adversaries will want to attack.

This paper contrasts two concepts: *cyber storm* and *cyber blitzkrieg.* The former has considerable currency for planning in cyber civil defence, the latter has little currency in any context−yet. The likely scope of conflict in cyber space is rapidly expanding, as the likelihood of it is also increasing. The paper's attention to blitzkrieg goes to a level of conflict one step beyond the cyber storm, as it was initially framed as the main focus of this research project. The difference is discussed below. Either way, storm or blitzkrieg, the planned scholarly volume from this project will be the first book-length effort to analyse a challenge identified for more than a decade but not researched as directly or as extensively as it might have been: civil defence against a national cyber crisis affecting national security.

For its own purposes, this paper poses the question of how states (great powers and middle powers) should plan for defence of the home front against the contingency of cyber blitzkrieg (including mass information war). The aim of such a cyber blitzkrieg will be to prevent the billion dollar weapons platforms of an enemy from reaching the front line of combat or (if they get there) to malfunction, to disrupt enemy command and control, and to disrupt civil sector support (including political support) to the enemy's armed forces.

Of special note, the very concept of home front has been transformed by globalization in general, and by the specific characteristics of cyberspace—especially the "anti-sovereign" entanglement in cyberspace of information and communications technology (ICT) that underpins daily life both on the home front (within a country's borders) and beyond (Pontbriand and Austin, 2019).

This paper sets out some research questions around the concepts of "civil defence" as they might apply to these extreme contingencies. The paper also looks to the emerging policy trends, where the United States is clearly leading. The paper briefly notes the impact on strategic policy of a cyber civil defence gap: highly vulnerable countries with little response capability will be constrained in shaping coercive pressure on potential adversaries. The paper provides a brief overview of the literature to date, building off a published literature review (Thakur 2016) of the research on dependencies in cyber space. That review confirmed a very low level of engagement, outside of three U.S. based-research centres, in the policy dynamics of cyber civil defence for extreme contingencies.

At the outset, to help readers make the leap to the future, the paper must state several likely assumptions:

- comprehensive protection of cyber systems (absolute cyber security) is not possible, far from it

- in matters of war between states, risk management approaches as practised in business in peace time (balancing cost benefits of investment in cyber security against cost of attack) will for most purposes in war time or a period of imminent war be irrelevant.
- The cyber security of a state is not the sum of the cyber security of its enterprises and government or military agencies, it is something very different. The sense of comfort that national cyber security planners may feel from helping enterprises improve their own security should not be imagined as constituting the greater share of national cyber civil defence.

A deeply analytical and forward-looking approach is needed, as suggested by Baumard (2017:73): "A national strategy for cybersecurity must not only be compliant with the global state-of-the-art of computer security R&D, it ultimately needs to anticipate scientific research and technological advancements that may either impede or transform its organization."

Cyber Storm

Cyber Storm is the name of a novel, a video game, many twitter users, and a U.S. company, all of more recent provenance than the exercise series by that name mentioned above that began in 2006. (A full set of cyber storm reports, to 2016, is available at https://www.dhs.gov/publication/cyber-storm-final-reports.)The first exercise was notable for several things:

- Exercised attacks on critical infrastructure in the USA but included disinformation operations to cloud assessments of the extent of the attack
- Led from computers in the U.S. Secret Service
- 115 participants
- Involved three U.S. states (Michigan, Montana and New York)
- Involved at least one leading private corporation (Microsoft)
- Did not involve major ISPs or internet backbone providers
- Involved the American Red Cross
- Included the Public Safety Ministry of Canada.

The scenario for Exercise Cyber Storm II in 2008 was "executed by persistent, fictitious adversaries with a distinct political and economic agenda. The Cyber Storm II adversary used sophisticated attack vectors to create a large-scale incident requiring players to focus on response." That set the directions for later exercises as summarized on the DHS website and as repeated verbatim in Box 1.

By 2018, DHS had identified the following objectives of its Cyber Storm exercise:

- examine organizations' capability to prepare for, protect from, and respond to cyber attacks' potential effects;
- Exercise strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures;
- Validate information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information; and

- Examine means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests.

Box 1: DHS Summary of Cyber Storm Exercises

- Cyber Storm I, 2006, was the first time the cyber response community came together to examine the national response to cyber incidents
- Cyber Storm II, 2008, exercised individual response capabilities and leadership decision making[1]
- Cyber Storm III, 2010, focused on response according to national-level framework and provided the first operational test of the NCCIC
- Cyber Storm IV included 15 building block exercises between 2011 and 2014 to help communities and states exercise cyber response capabilities for escalating incidents
- Cyber Storm V, 2016, included more than 1,000 distributed players and brought together new sectors including retail and healthcare participants
- Cyber Storm VI, in 2018, focused on "critical manufacturing and transportation sectors, with participation from the information technology and communications sectors; law enforcement, defense, and intelligence agencies; state and local governments; and international partners"

Of some note, as early as Cyber Storm II in 2009, DHS concluded that "through the interaction between the public and private sectors, the exercise accurately simulated the interdependencies of the world's cyber and communications networks".

Thus the DHS conception of cyber storm appears to fit the official US definition of "Significant cyber incident", one "that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people". This formal definition was promulgated by President Obama (White House 2016) and reiterated by President Trump in the May 2017 Executive Order (White House 2017).

The definition fits with one used by the Resilience Systems Grand Challenge team at Idaho National Laboratory (INL), one of only a small number of leading centres in the world for the scholarly study of serious cyber critical infrastructure threats at the national level. INL (Stacey B. 2015) says it is possible to identify three tiers of national level response to cyber security in the broad, and that INL does not research the first tier:

- Hygiene: cyber security practices
- Advanced persistent threat: "the more sophisticated criminal and nation state persistent campaigns"; requiring "a strategic partnership with industry and government"; "these roles are still evolving"
- High impact low frequency events: "catastrophic and potentially cascading events that will likely require substantial time to assess, respond to, and recover from."

The INL resilience program assumes pervasive insecurity. It rejects "traditional trust relationships in peer communications" and "expects a malicious actor or actions to be part of

normal operation" and is designed to mitigate such actions". It promotes "a paradigm shift in the methods used to historically develop control systems" (INL website 2016).

Few governments have developed the cyber storm concept beyond the DHS exercises. One exception is Australia. In November 2016, the country's Cyber Security Minister, Hon. Dan Tehan MP, made a ground-breaking speech at the National Press Club (Tehan 2016). He warned the country to be prepared for a cyber storm. The speech represented a reversal of previous government policy of understating cyber threats at the national level in order to avoid arousing undue anxiety among the population. This policy had been actively opposed by some government advisers, and with the installation of the first Minister dedicated to the portfolio just months earlier, the cyber realists got their way.

Tehan sketched a scenario:

- "power goes out across a large part of one of our capital cities
- street and traffic lights fail; mobiles without reception and landlines dead
- a [power surge] has damaged energy generators that feed into the power grid
- coordination efforts grind to a halt as any communications infrastructure … is overloaded with demand
- chaos reigns as people panic, leading to damage and loss of life
- local businesses must revert to cash; ATMs are inoperable
- It takes weeks for the power to be turned on in some areas. Meanwhile the local economy is frozen".

Tehan proffered the cause of this hypothetical situation to be an attack against a power company by a cyber virus introduced to their systems through a subcontractor: "Someone had opened an email, looked at a document, and sent the system into meltdown".

This scenario posits catastrophic cascading effects from a single vector, one-off cyber attack.

Thus we can say with confidence that the term "cyber storm" has a demonstrated appeal in at least several countries for key stakeholders as a vehicle for organising national-level responses to severe cyber crises. The concept as used is not precisely defined, nor legally defined. While closely linked to the contingencies of major warfare in cyber space, the concept "cyber storm" maintains a high relevance to non-military planning for high end contingencies in peacetime or in wartime. One of the primary benefits of "cyber storm" as a term of art may be as a vehicle for policy mobilisation for new forms of civil defence that will likely involve in significant ways the non-cyber emergency management agencies in most countries.

The concept is worth a little further reflection on at least two points: local aspects and frequency/concentration.

Local Attacks, National Effect

First, like its natural namesake, a cyber storm will have localised effects and identified localities even if it has national impact. The "cyber storm" will in many cases manifest itself as a series of unrelated local storm systems, occurring differently in any of ICT infrastructure and affecting cyber resilience. Australia's former Prime Minister, Malcolm Turnbull, went so

far as to affirm this point about multiple storms by reference to the popular disaster movie, *Perfect Storm* (Turnbull 2018).

Specialists at Bell Labs identified eight ingredients of cyber security, five of which are more technical (hardware, software, payload, networks, electricity supply) and three of which are more non-technical (people, policy, and ecosystems) (Rauscher et al 2006). In planning for the cyber storm, it will be important to understand these three non-technical aspects, a proposition captured well enough in scenarios and conduct of the U.S. cyber storm exercises. What has been less explicit in these scenarios is the impact of the local social factors that interact in unique ways with the national scene: "local" policy, "local" people, and "local" ecosystems".

The proposition that infrastructure itself can "channel" cascading consequences (Pescaroli and Kelman 2017) is highly relevant here. The unique ways in which localities have been configured or operate will impose additional complexities in a cyber storm. This is well illustrated by the power supply chaos that followed a severe natural storm event in South Australia where the (computerised) tolerance settings of individual wind turbines[1] were neither mapped nor understood for their impact on load shedding of the network (AEMO 2017: 6).

The centrality of local (or regional) considerations has led to the emergence of regional bodies or mechanisms to respond to the needs. In the case of the United States and Australia, this can be seen in the creation of Chief Information Security Officer posts in all states[2] (though the practice is far from standardised as to mission sets, with some emphasising privacy concerns as much as system security and resilience). In the United Kingdom, a privately-led initiative to establish "Cyber North" based around Newcastle was an important if modest development, following the success of a limited role for an organisation called London First in that city in cyber emergency preparedness.

One Storm or Many?

Second, as I have argued elsewhere, a cyber storm—were it to be unleashed by one state on another—would be more likely to be multi-vector (using cyber arsenals, hundreds of "tools"); involve polymorphic malware (APTs); be multi-wave (sustained); multi-locality; involve civil and military targets; affect intended (strategic) targets and accidental, unintended targets; be accompanied by targeted social influencing (information campaigns); and for all of that, have unpredictable as well as predictable cascading effects (Austin 2016). Table 1 below provides examples of known or contemplated attacks that any determined state actor would at least consider in preparing a cyber storm against another. This approach was used by Seinor (2015) in discussion with the author and has been updated by the latter. Though the U.S. government predicts cyber storms of such severity, its exercises under the rubric have not contemplated such complex, multi-faceted onslaughts on a rolling basis over protracted periods.

---

[1] "All SA wind turbines have a [software] control system that takes action if the number of ride-through events in a specific period exceeds a pre-set limit. If the pre-set limit was exceeded in the event, each wind turbine either disconnected from the network, stopped operating (remained connected with zero output) or reduced its output. The pre-set limit varied from wind farm to wind farm, and some were set low enough for the six voltage disturbances in the event to exceed their limit."

[2] The Australian state of Tasmania was unsuccessful in filling the post after a year-long search. [check current situation]

Table 1: Examples of Options to Include in a Cyber Storm

notPetya ransomware attack 2017
China's kinetic anti-satellite test 2007
Stuxnet 2010 (cyber sabotage against SCADA)
release by the group Anonymous of military personnel data
cutting of undersea cable (numerous incidents)
closing down of civil satellite links (Egypt)
closing down electric grids by cyber attack (U.S. in Yugoslavia 1999)
insertion of false data into military systems (Iranian hijack of U.S. drone)
Iranian attacks on Saudi Aramco 2012
Iranian attacks on US banks 2012
planting malware in civil aviation systems (2010 international treaty criminalising it)
opening flood gates on dams or attacking nuclear power stations (US laws of war 2015)
closing down adversary's civil communications

Cyber Blitzkrieg: Timing is Everything

The future is looking very different. Scholars debate the political utility of single cyber weapons, but few imagine how the political utility of a cyber weapon may be transformed when it sits among arsenals of such weapons, and where states craft war-fighting doctrines around multi-vector, multi-wave, pre-emptive and sustained cyber campaigns of the sort just mentioned.

And in 2019, we are still at the dawn of the cyber age. What will cyber arsenals look like between 2030 and 2060? What will the technical modes and vectors of cyber attack look like in that time frame? Will cyber attacks be deliverable by radio signal to air-gapped systems? How will states plan to use their cyber arsenals? The concept of cyber blitzkrieg has not been widely articulated by scholars nor has it been formally adopted by any state in its military or strategic planning. But it would seem highly likely, if not inevitable.

What does the concept of *blitzkrieg* (meaning in English "lightning war") bring to the subject of this paper?

There are competing interpretations of the subject well captured in the book, *Blitzkrieg Legend*, by a German researcher and first published in 1966 in German (Freiser 2013). He lays out several early uses of the concept at the time of the First World War, mainly at the tactical and operational levels of combat and involving assault units, highly mobile tactics and forces operating at speed. When it comes to the strategic level of war, Freiser shows convincingly that the concept was never official German military policy but rather it was a term used several times by military writers between 1935 and 1940 and one that gained foreign prominence after the surprise German victory in its Western campaign against Belgium, France, and Allied forces in those countries in 1940. The 1935 use of the term in German, by a military author described by Freiser merely as von Schichow, is quite close to how the English term came to be understood, as a strategy "to finish a war quickly and suddenly by trying to force a decision right at the very beginning through the ruthless employment of their total fighting strength". Von Schichow suggested this strategy was appropriate for states "with a rather weak food industry and poor in raw materials". A 1938 German military writer talked of blitzkrieg as "strategic surprise attack", using armour, air forces and airborne troops. But Freiser also

documents the dominant thinking in the German High Command prior to 1939 that the very idea of a quick short war was folly, one that had dominated the failed strategic vision of Germany in the First World War, when strategic thinkers favoured an offensive strategic posture (Posen 1984, Snyder 1985).

The first claim about the relevance of the term *blitzkrieg* to cyber conflict is that these weapons are the only ones, alongside classic electronic warfare weapons, ever invented that can be delivered at truly "lightning speed" (*der Blitz* in German means "lightning".). This has important connotations for strategic preferences between defensive strategies and offensive ones, a view that has been well researched and analysed in scholarly literature (summarised well by Slayton 2017), including the very important concept of pre-emption (Austin and Sharikov 2016). The essence of the well-studied and supposedly "inherent" propensity for offence in cyber operations is the idea to force a war outcome "quickly and suddenly … right at the very beginning through the ruthless employment" of cyber assets (rather than a country's "total fighting strength", to use von Schichow's words from a pre-cyber era).

At least one country, the United States, is planning, in wartime to be able to conduct offensive cyber operations in all phases of operations and at all levels of command. This concept includes attacks on civil infrastructure related to the war effort, including—in the event of military necessity—possibly against civil nuclear power stations and dams. That country has already accumulated arsenals of different cyber weapons to enable multi-vector, multi-wave, pre-emptive and sustained attacked an on adversary's military and civil infrastructure in extreme contingencies.

Civil Defence: A Contested Space

In a book written about civil defence policies in response to the threat of nuclear war, Vale (1987: 1) described the idea of civil defence as both unpopular and unsettling. While in peacetime, the burdens of thinking about the subject can be assigned to political leaders (as to bureaucrats and academicians), Vale notes that the burdens of implementation of civil defence measures in peace and war "are physical" and that they "directly influence the daily lives of every citizen". He talks of the two poles of the debate: on the one hand, most commentators will always judge a civil defence plan to be inadequate, and on the other, the very fact of such planning can be "censured … for representing an excess of state control". The concept of civil defence is controversial, because it is inherently political and because it forces the state's choices and needs on private actors. But it is also controversial because of how some of the historical instances of the practice played out in the politics of the day. Civil defence is a concept often used by dictators to justify death squads or other extra-judicial killings.

The modern concept of civil defence has been traced by some researchers to the First World War, when aerial bombing campaigns began producing psychological shocks on civilian population (DHS 2006: 4-5). But the concept was at the root of revolutionary movements and political revolt: protection of civilians against repressive regimes through formation of civilian militias. The term "civil defence" in English was recorded as early as 1758, according to the Collins English Dictionary. In the American Revolutionary War, militias formed for purposes that included civil defence. In 1789, revolutionary militias were formed in Paris for civil defence. In French, one cognate term, *la protection civile* (civil protection), has additional connotations of popular defence that the English term in current usage has lost. In German, the term *zivilschutz* (civil protection) has a vibrancy and contemporary legitimacy, largely because of the practices in Switzerland, not common in many English-speaking countries. In 2016,

Germany issued new regulations on civil defence (*Zivile Verteidigung*) to prepare for a possible armed attack or natural disaster. In the Arab Spring (Tunisia and Syria), as in some of the West African conflicts in the 1980s and 1990s, militias also formed for civil defence. The term in Russian (*grazhdanskaia oborona*) is a simple translation of the English equivalent, though it carries of a stronger connotation of citizen involvement. The Chinese term (民防 or *mín fáng*) and its use in China and Taiwan implies citizen involvement in national defence, as well in government responses for natural disaster.

Today, the term "civil defence" can mean several different things:

- Organized defensive measure by civilians and/or the state to protect civilian populations in wartime or other emergencies, such as natural disaster
- Actions by civilians in support of military defence and war objectives
- Actions by civilians in opposition to the state to protect the people from state abuses (people's self defence)
- Actions "to mitigate the loss, damage and suffering inflicted on civilians as a result of the dramatic development of the means and methods of warfare. It is an essential component of the protection of civilians against military operations provided by international humanitarian law" (ICRC defintion).
-

This paper is focused on the activities covered by the quite broad definition in the Oxford Dictionary: "The organization and training of civilians to be prepared for attacks in wartime". For this author, that definition also includes preparation for national emergencies just short of war. At the roots of this meaning, civil defence is as much about psychological responses and resilience of the general population and the private sector economy as it about the direct contribution of the civil sector to conduct of war. This definition does not preclude measures involving civilians to support military responses by the state.

In 1958, the International Civil Defence Organisation (ICDO) was established as a rebadging of the former International Association of Geneva Zones set up in 1931. ICDO has 58 member states, none of them are OECD countries, and the current Director General is a Russian citizen. France and Portugal have observer status. Many countries (including for example New Zealand) have civil defence ministries which are responsible for emergency and disaster response, as well as other non-specified contingencies.

Civil defence was accorded a new international legal status and defined in Article 61 of the First Additional Protocol to the Geneva Conventions of 1949 relating to the protection of victims of international armed conflicts, as set out in Box 2 (United Nations Treaties 1979).

Civil Defence organisations operating in a combat zone are entitled to the same protection as humanitarian agencies. To aid in this. there is an internationally recognised symbol for civil defence: 'an equilateral blue triangle on an orange ground', as described in Article 66(4), and used as the basis for the logo of the American Civil Defense Association (figure 2).

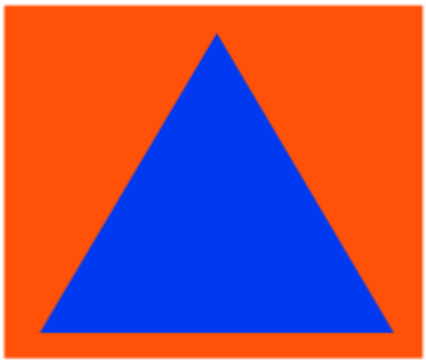

Fig 1: Symbol for Wartime Distinction of Civil Defence Facilities and Personnel

Fig 2: Logo of the American Civil Defense Association

Box 2: Geneva Protocol Definition of Civil Defence Tasks

"the performance of some or all of the undermentioned humanitarian tasks intended to protect the civilian population against the dangers, and to help it to recover from the immediate effects, of hostilities or disasters and also to provide the conditions necessary for its survival. These tasks are:
(i) Warning;
(ii) Evacuation;
(iii) Management of shelters;
(iv) Management of blackout measures;
(v) Rescue;
(vi) Medical services, including first aid, and religious assistance;
(vii) Fire-fighting;
(viii) Detection and marking of danger areas;
(ix) Decontamination and similar protective measures;
(x) Provision of emergency accommodation and supplies;
(xi) Emergency assistance in the restoration and maintenance of order in distressed areas;
(xii) Emergency repair of indispensable public utilities;
(xiii) Emergency disposal of the dead;
(xiv) Assistance in the preservation of objects essential for survival;
(xv) Complementary activities necessary to carry out any of the tasks mentioned above, including, but not limited to, planning and organization.

Vale (1987: 4) advocated a comparative approach to study of the subject of civil defence. Noting that each state has its own situational logic and unique responses, one value in comparative analysis is that it allows the researcher to discover what type of practices might be more effective in certain types of states. Starting from the proposition that civil defence against nuclear war would always be inadequate, his research goal was to establish the ways in which the technical limitations might influence policy. This is a useful guidepost for the current research.

In the late 1970s, civil defence rose to the top of the U.S. political agenda when arguments surfaced suggesting that Soviet leaders might be more likely to consider the utility of nuclear war because their civil defence system was far better developed than that of the United States. For a summary of this argument, see Garrison (2007). This was called the "civil defence gap", so called for its similarity to previous gaps in the national military capability of

the two countries: the bomber gap in the 1950s, the missile gap in the 1960s, and the European theatre's conventional forces gap in the 1970s. In 1978, the CIA responded to the public debate by publishing a Top Secret assessment rejecting the argument about the strategic implications of that particular civil defence gap (DCI 1978). There were however important observations about the potential of civil defence capabilities to shape strategic policy: "Civil defense in the Soviet Union is an ongoing nationwide program under military control. The Soviets' strategic writings integrate civil defense into their military strategy." The report also concluded that "By developing an active and extensive civil defense, in conjunction with their other defensive and offensive strategic programs, they [the Soviets] hope to convince potential enemies that they [cannot go to][3] war with the USSR. If war should occur, the Soviets seek through civil defense along with other means to assure survival of the homeland and to leave the USSR [in a] stronger postwar position than its adversaries". The CIA authors reported that despite a clear commitment by the Soviets to a uniformed civil defence force, its effectiveness was degraded by bureaucratic difficulties and apathy amongst the population.

In fact, the weight of scholarly and expert opinion at the time was that there was no "nuclear war civil defence gap" of the sort that the more extremist analysts had suggested, which they had claimed could alter the Soviet strategic calculus about the utility of nuclear war.

Thus the lessons for this paper, both from Vale's book and from the brief mention of the Soviet case, is that civil defence gaps are commonplace and may not have such dire consequences as their mere existence might suggest. But put differently, if we want to claim dire consequences about civil defence gaps we need to demonstrate the likelihood of such consequences beyond merely asserting them. In the case of cyber civil defence, high grade and complex simulations of cyber storm or cyber blitzkrieg would appear to be an essential tool.

Cyber Civil Defence: A Fast Moving and Contested Catch-Up Challenge

Specialists, governments and business leaders in many countries agree that a catastrophic cyber emergency is highly unlikely in peacetime but they cannot agree on what priority to accord it in national strategies. Several governments, especially the United States and Estonia, view the threat as credible and have accorded such a possibility a high priority in their planning. This approach of preparedness conforms to the traditional approach that while outright war with major powers, like China and Russia, is highly unlikely, it is still essential to have defence capabilities in place, as well as mobilisation plans, for the eventuality. The need to plan for extreme cyber emergencies is not only driven by the common dictates of national defence policy, but the unique characteristics of cyber space and vectors of attack or system failure within ICT infrastructure. The need has also been fuelled by the more recent attention accorded to hybrid warfare, especially hostile acts that might fall below the level of armed conflict as defined by the Laws of Armed Conflict, and other sources of law on war and peace.

The policy commitment today to cyber civil defence is buttressed by confidence that it is plausible and viable, in strong contrast to the view in much of the Cold War that civil defence against nuclear attack was probably a waste of time. (One clear exception to that was the plan of protecting a country's highest level leadership and ensuring the continuity of wartime

[3] The document reference for this paper was only available in a text automatically general from an OCR scan of the original. So there are some inconsistencies and errors in the web version. This author has reconstructed a small amount of garbled text to the insert the words "cannot go to" and [in a].

political command authorities). Given the common belief that cyber civil defence is viable, it is useful to consider its evolution. The following discussion concentrates on the United States since it has been the clear leader in the field.

The country strongly articulated a need for cyber civil defence as early as 1998, though as part of a much broader agenda of national security reform. According to one source, it was in 1998 that DARPA set up its first research project on network security from the perspective of resilience of critical cyber infrastructure (Baumard 2017: 48). It was also in 1998 that the international community took the first steps toward possible collective preparations for common civil defence when the UN General Assembly supported a Russian drafted resolution on Developments in the field of information and telecommunications in the context of international security. The United States co-sponsored the resolution along with other states. That year, cyber security was one of a long list of agenda items approved by Presidents Clinton and Yeltsin for bilateral development (Gady and Austin 2010:1). The Hart Rudmann Commission, set up in 1998 and chaired by Secretary of Defense William Cohen, recommended in its final report published in early 2001 the creation of a National Homeland Security Agency charged with novel and wide-ranging responsibilities for cyber space and CIIP (Hart Rudmann 2001). The 2001 report leaves the reader with an impression that in spite of much change in the years since, the same over-arching challenges remain in place. It talks of cyber workforce shortages, need for better private/public interactions, advanced cyber situational awareness, and early warning. Of course, what happened was that policy did respond to some degree but the threats did not stand still.

By 2003, Justice and Interior Ministries of the G8 countries adopted Principles for Protecting Critical Information Infrastructures" (G8 2003). The principles can be read as an affirmation of the need for classic cyber security at the enterprise level, but they stray very far into traditional areas of civil defence without using that term. The preamble asserts a national level responsibility for protecting critical information infrastructures (CII). This should include, the document said, country-wide threat identification, vulnerability reduction, damage minimization, fostering speedy resilience, and investigation for criminal prosecution. The measures should involve "communication, coordination, and cooperation nationally and internationally among all stakeholders -industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies." The document included privacy protection and continuing security of sensitive information as guiding considerations. There were two simple principles: "countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents"; and "countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them".

The G8 principles provide a basic checklist for evaluating subsequent national cyber civil defence plans. No G8 member has successfully implemented these principles in a comprehensive fashion. They were almost certainly adopted under the strong influence of the United States, though perhaps with most other governments not really being as convinced as the Americans of the need or the urgency.

By 2005, the U.S. government had committed itself to a six-point plan for SCADA protection against terrorist attack which involved the following elements (Purdy 2005), verbatim:

1. Establish a National Cyberspace Response System to prevent, detect, respond to, and reconstitute rapidly after cyber incidents

2. Work with public and private sector representatives to reduce vulnerabilities and minimize severity of cyber attacks
3. Promote a comprehensive awareness plan to empower all Americans to secure their own parts of cyberspace
4. Foster adequate training and education programs to support the Nation's cyber security needs
5. Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace
6. Build a world class organization that aggressively advances its cyber security mission and goals in partnership with its public and private stakeholders.

By 2005, Sandia and Idaho National Laboratories had begun serious work on SCADA vulnerabilities and mitigation strategies, and the DHS was already working with leading non-American corporations with a global footprint, such as Siemens and ABB.

At around this time, in 2006, Idaho National Laboratory began conducting research on precursor subjects (Dudenhoeffer, Permann and Manic 2006) to its later Grand Challenge on National Resilience. This Grand Challenge would address the "catastrophic and potentially cascading events that will likely require substantial time to assess, respond to, and recover from" (INL website 2016). Dudenhoeffer at al concluded (p.482) that "very few models exist that seek to tie these [different] infrastructures together in a form representative of their actual implementation. Additionally, many of these models present a physics/engineering-based approach and are very good at individual sector analysis, but they do not necessarily support high level command and control."

In 2009, the Department of Homeland Security (DHS) made a globally significant innovation in policy. It devised a ten-point plan for cyber resilience (DHS 2009) and offered the country's corporations the service called Cyber Resilience Review (CRR) based on ten elements:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness

This process was heavily oriented toward the enterprise level as well as to technical aspects of cyber security classically defined, but it remains of enduring relevance to national-level CIIP policy preparedness for a cyber storm (complex cyber emergencies of a national scale).

In 2010, researchers at Sandia National Laboratory (Keliiaa and Hamlet 2010) warned of seven structural defects in U.S. decision-making that would undermine its resilience in an extreme cyber emergency. These priority problems, listed verbatim, are:

1. disjointed response to wide-area and multi-target attack
2. widely dispersed and fragmented detection and notification capabilities

3. ill-defined government, commercial, and academic roles and responsibilities
4. divided and rigid wide-area cyber protection posture
5. unresolved wide-area common and shared risks
6. fragile interdependent wide-area critical access and operations
7. unresolved attribution of attack and compromise.

The Sandia paper lays out a future "technology of decision-making" based on high performance computing that might usefully be understood by analogy as an attempt to create for cyberspace, as a global civil domain, an up-scaled version of the global strategic C4ISTAR system for U.S. command of its strategic nuclear weapons, including indicators and warning.

The study took as a core operating principle the proposition that the cyber security terrain for national decision-making is a "continuous lifecycle with human, organizational, legal, and technical interdependencies". It identified seven high priority "wide-area problems" in the field of cyber security that have high relevance to middle powers in understanding its technologies of decision-making for cyber-enabled war. The authors concluded by recommending areas for further research in high performance computing to support national security decision making for cyber space.[4]

In 2011, President Obama signed PPD 8 on national emergency preparedness, including for nationally significant cyber attack (DHS 2011).

By 2015, INL–while committed to a Grand Challenge in national cyber resilience–was losing confidence. In testimony to Congress, a senior official made several key observations (Stacey 2015):

- The presumption that a control system is "air-gapped" is not an effective cyber security strategy. This has been demonstrated by over 600 assessments.
- Intrusion detection technology is not well developed for control system networks; the average length of time for detection of a malware intrusion is four months and typically identified by a third party.
- The dynamic threat is evolving faster than the cycle of measure and countermeasure, and far faster than the evolution of policy.
- The demand for trained cyber defenders with control systems knowledge vastly exceeds the supply.

In both 2015 and in 2016,[5] President Obama twice declared a national emergency in cyberspace demanding dramatic changes in U.S. readiness. Obama also issued an Executive Order on National Cyber Incident Response (White House 2016).

The signal for a CIIP revolution came in May 2017, when President Trump signed the Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (White House 2017).

The Trump order was a declaration of war on the technological and procedural lock in of the national cyber security establishment: "The executive branch has for too long accepted antiquated and difficult–to-defend IT". It called for a new integrated and comprehensive

[4] These areas for research were: trusted connection and automated processes; informatics, statistics and anomalous behavior; mathematics analysis and intrusion detection; complexity science and emergent behavior; modeling and simulation; analysis and correlation algorithms; sociology and psychology.

[5] The legal term of a national emergency is no longer than one year, so in April 2016 the President had to renew it.

approach: “Effective risk management requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources”. It mandated that all federal agencies would use the “Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology, or any successor document, to manage the agency’s cybersecurity risk”. It brought about a shift in the public/private balance in CIIP: “It is the policy of the executive branch to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation’s critical infrastructure”. This did not mean that the government would support incident management inside the operators’ systems.

It did go one step further: it called on federal agencies to “identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified … to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security”.

It called for special attention to the electricity sector, asking agencies to study the “potential scope and duration of a prolonged power outage associated with a significant cyber incident, …. against the United States electric subsector; the readiness of the United States to manage the consequences of such an incident; and any gaps or shortcomings in assets or capabilities required to mitigate the consequences of such an incident”. It also called for an assessment of defence readiness for war-fighting through an additional study of “cybersecurity risks facing the defense industrial base, including its supply chain, and United States military platforms, systems, networks, and capabilities, and recommendations for mitigating these risks.”

The Trump Executive Order was an attempt to shatter the pre-existing pattern of complacency and incremental policy change. It called for national and democractised cyber security revolution that recognised both enterprise level challenges and the cyber storm challenge. The central place of new research in this paradigm shift was one of its chief features. The President called for a raft of studies to be presented in short order and others to be a continuing process. The list of completed studies is available on the DHS website (DHS 2018a). It includes:

- Report to the President on Federal IT Modernization
- Support to Critical Infrastructure at Greatest Risk
- Supporting Transparency in the Marketplace
- Resilience Against Botnets and Other Automated, Distributed Threats
- Assessment of Electricity Disruption Incident Response Capabilities
- American Cybersecurity Workforce Development.

It is notable that in the period around the time the Executive Order was issued, the Pentagon was undertaking major reviews of the national security strategy and associated military doctrine, premised on part on a reassessment of the serious of the cyber threats to the United States. The new National Security Strategy (NSS) was issued in December 2017 (White House 2017b), and several revised doctrine manuals were issued between April and July 2018. (For a summary of the doctrine revisions see, Austin 2018a.)

The new NSS had lengthy treatment on "keeping America safe in the cyber era" inside its Pillar 1 (Homeland Defence) and included measures already flagged in the Executive Order. The NSS (12-15) specifically committed the government to the following key initiatives for CIIP:

- Identify and prioritise risk
- Disrupt and deter malicious actors
- Incentivise and improve information sharing and sensing
- Deploy layered defence.

Of special note, the NSS described at length the centrality of the population at large in ensuring national cyber resilience in extreme contingencies (15). This sentiment is not share in most jurisdictions in the world.

Of the Pentagon documents released in 2018, the strategy note (DoD 2018) is of most interest. It supplements three earlier Joint Chiefs' doctrines on military policy, joint operations; and joint planning. It is not intended to be authoritative but rather "provides context for those who develop national strategy and implement it at subordinate level". The note does not refer to cyber space as a fifth domain of warfare, but refers to "any domain (land, maritime, air, space) and the information environment (to include cyberspace)". This must be a fundamental point of strategic reorientation for all countries' armed forces. Cyber space is not in the U.S. Joint Chiefs' view a fifth domain of warfare but an environment shared by the commonly known four domains.

The update on cyber, *Cyberspace Operations* (JCS 2018a), replaces the 2013 joint publication and provides new guidance on the command and control of cyberspace operations and their planning. One of the big changes is the distinction between two modes of command and control for cyberspace operations: "routine and Crisis/Contingency". An important feature of this section for U.S. Allies is recognition that a military alliance in cyberspace will look and operate differently from other forms of cooperation: "the level of integration of US cyberspace forces with foreign cyberspace forces will vary depending upon in-place agreements with each partner and may not mirror the level of integration of other types of forces".

One of the more ground-breaking documents is the update of *Homeland Defense* (JCS 2018b). It specifically recognises the role of Cyber Command in homeland defence missions, and assigns Special Operations Command a primary responsibility for coordinating cyber missions against terrorists in U.S. territory. It also asserts a new mission of coordination with the private sector for cyber homeland defence operations involving U.S. military forces: "For cyberspace, the vulnerability and complex interrelationship of national and international networks demand closely coordinated action among the military, private sector, and other government entities at all levels."

On the international stage, while the UN resolution first introduced in 1998 and referred to above has had a chequered and politicised history involving occasional stand-offs between the two cyber blocs (United States and its allies against China, Russia and their like-minded countries), the resolution did lead ultimately to a consensus in 2015 in the Group of Governmental Experts (GGE) on possible voluntary norms regarding common civil defence measures in cyber space, as listed in Box 3 (UNGA 2015). This process was also one on which the United States played a driving role, a fact that led subsequently to several governments walking away from or muting their support for the 2015 consensus.

BOX 3: Selected Possible Voluntary Norms Agreed by the GGE in 2015

A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.
States should take appropriate measures to protect their critical infrastructure from ICT threats.
States should take reasonable steps to ensure the integrity of the supply chain, so end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions."
States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities, in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

The work by the GGE stimulated the creation of the Global Commission on Stability in Cyberspace (GCSC), which also took up issues of common (global) civil defence, including protection of the backbone servers of the internet.

Some leading private sector organisations also began to accord a high priority to planning for extreme cyber emergencies. For example, in 2013, a global survey by the World Federation of Exchanges (WFE) and the International Organization of Securities Commissions (IOSCO) found that 89 percent of respondent exchanges considered that cyber crime in securities markets can be considered a systemic risk. It continued to develop policy responses and in November 2015 advised its members to plan for "extreme but plausible scenarios". In 2014, the Bank of International Settlements (BIS) called attention to the threats and risks in cyber space inherent in financial market infrastructures: "their biggest cyber vulnerability is managing their complexities and interdependencies" (BIS 2014). Other international organisations, such as the International Atomic Energy Agency (IAEA) and the international Civil Aviation Organisation (ICAO), also undertook important initiatives for CIIP in their fields beginning in 2102 at least for IAEA (Austin et al 2014) and later, in 2017, for the ICAO. Although in the case of ICAO, it should be noted that the members had supported a new treaty in 2010 (Beijing Convention) that inter alia criminalised "technological attacks" on aircraft or air traffic control, a term specifically understood as including cyber attack (Austin et al 2014).

The intensity of such responses continues to gather steam but have yet failed to instil confidence. For example, a survey of 450 companies worldwide in 2018 by the Economist Intelligence Unit and Willis Towers Watson found that there was little consensus on resilience measures and planning, underpinned by a pervasive lack of confidence in the availability of all the people needed to deliver the outcomes (Insurance Journal 2018). In 2017, a report by the U.S. President's National Infrastructure Advisory Council (NIAC 2017:5) found that the country was falling short in the mission of CIIP. Of special note, the report also found that cyber civil defence was plausible and viable: "the Council (NIAC) believes that the federal government and private sector collectively have the tremendous cyber capabilities and resources needed to defend critical private systems from aggressive cyber attacks—provided

they are properly organized, harnessed, and focused." Whether other countries share this confidence is open to debate.

In a 2018 survey of the 50 state CIOs/CISOs/CSOs or their equivalents in the United States, Deloitte and the National Association of State Chief Information Officers (NASCIO) found that in spite of great "strides in governance and in establishing the CISO role's legitimacy", these actions "have not resulted in significant progress in overcoming the top challenges US states face in implementing effective cybersecurity programs". The report cited "perennial challenges in acquiring an adequate budget and workforce to carry out their responsibilities". The report did not have the illusion that states and business leaders would necessarily be in a position "to fully address these hurdles", but the authors advocated for a "concerted effort to close the gap lest it widen even further" (Deloitte and NASCIO 2018:3). There were three main recommendations (p. 4):

1. Cyber legislation equipped with funding to advance state cyber risk programs
2. Federal funding to meet mandated federal cyber requirements
3. Public-private-academia partnerships to overcome persistent talent gap issues and improve service levels in security functions delivered

There are credible studies suggesting that all countries, including major powers like France (Baumard 2017), China (Austin 2018b), India (Sharma 2019), and the UK (Joint Committee 2018), face similar shortcomings in cyber civil defence and for similar reasons of technological vulnerability and late start at policy remedies. In the case of China, for example, a senior PLA engineer commented in 2014 that "Compared to the massive and frequent nationwide 'Cyber Storm' exercises that the United States held in recent years, China falls far behind both in scale and in technical levels" (Xinhua 2014). This assessment is supported by more recent scholarly analysis (Austin 2018b; Sharma 2019) that sees China as quite backward in national CIIP planning.

Thus between 2015 and 2019, there has been a tectonic shift in the urgency and character of civil defence planning for the cyber storm in several countries. We have now reached the point where the world's greatest cyber power states publicly that there is an arms race in the domain. These statements flow from findings that the country's civil defence in cyber space is not only seriously deficient but that these deficiencies can be remedied in a way that will contribute to the overall strategic power and military deterrence of the United States.

China, the rising cyber power, but one which is much weaker in cyber defence than the United States (Austin 2018b), has moved with considerable haste beginning in earnest in 2015, and staking its vision of national security on cyber security. President Xi said "there can be no national security without cyber security" and the country's 2015 Military Strategy that "outer space and cyber space are the new commanding heights of all international security competition". These statements imply that key states see existing cyber civil defence gaps, as having a significant impact on strategic policy. They believe that such a gap will constrain highly vulnerable countries with little response capability in shaping coercive pressure on potential adversaries. Countries that are the less vulnerable in cyber space such as North Korea may be more emboldened to aggressive action.

On the other hand, this negative trend also creates incentives for moves toward common security in cyber space. The idea of "international" information infrastructures is already afoot, as indicated above in reference to the GCSC work on protecting the core (backbone servers) of

the internet. In 2007, the U.S. government become concerned about such international dependencies in a range of critical infrastructures, including ICT-related, and set up the Critical Foreign Dependencies Initiative (CFDI). As part of this process it asked its embassies to report on those facilities in their host country that might be considered critical for the national security or economic prosperity of the United States. Based on the responses, the Department of Homeland Security compiled a prioritised list of these dependencies which included "over 300 assets and systems in more than 50 countries" (DHS 2008). In many cases, the landfall stations of the undersea cables in foreign countries were included, as were other telecommunications infrastructure. But at that time and since, as Arce (2015: 9) points out, there has been little consistent analysis of the character of the vulnerabilities and risks−what I would call the dependencies. He also notes an "absence of cyber entities in the list" (Arce 2015:10). The main enduring significance of this list might be that it highlighted the "discontiguous and non-traditional character" of U.S. vulnerabilities. The idea of international CIIP however was boosted in 2009 by work of the EastWest Institute on common understandings of the maintenance planning for global undersea communications cables (EastWest 2010) and by the news from Wikileaks that the U.S. State Dept that year had called on all of its embassies abroad to identify infrastructure in their host country that might be regarded as critical to U.S. national security or economic prosperity in the same ways of it were in U.S. territory.

Scholarly Views on The Turning Point

Academic research on these subjects has been voluminous but it has mainly concentrated on two broad areas. The first could be described as studies of cyber-enabled war, imminent war or the high politics of hybrid campaigns, including deterrence challenges. The second is a lower level of analysis, addressing technical aspects of infrastructure interdependency. The focus in this paper sits in relatively unoccupied middle ground. It reaches back to recover as a unique topic of investigation the original concept of "cyber storm": that is planning of defence by governments and corporations for the contingency of mass attack on critical infrastructure undertaken by an adversary for political or economic gain, with the hope of remaining below the level of armed conflict. This subject is being hotly debated in Track 1.5 discussion between the United States and China. (There are no such meetings in place between the United States and Russia.) There is little published research on the political dimensions of the problem set. The work of specialists on the first and second Tallinn manuals on the laws of armed conflict and other international laws applicable to lower levels of conflict in cyber space are highly relevant, but the social science research on the "cyber storm" as a driver of policy has not been so prominent. Most importantly, the cyber storm has rarely been studied by scholars from the point of view of the gaps in "civil defence". The best scholarly research broadly on this topic comes from the Idaho and Argonne National Laboratories, and Carnegie Mellon University, all in the United States.

A seminal article in 2009 called out what it saw as hyper-securitisation of cyberspace and over-exaggeration of threats (Hansen and Nissenbaum 2009). The authors saw room to challenge both an undue securitization and a possible Western bias (away from human rights and favoring the international security interests of the state). This article set the tone for some damping down by scholars in the years following of the serious of potential future threats in cyber space.

By the end of the first decade this century, there was a growing awareness that attacks on CII could possibly produce serious economic shocks, definitely at the national level and possible at the international level. As part of a series of five OECD case studies on potential

global shocks, the agency commissioned a report on whether a such a shock could be caused by a cyber attack (Sommer and Brown 2011). The authors concluded that "very few single cyber-related events have the capacity to cause a global shock" and that "it is unlikely that there will ever be a true cyberwar" (6). They assessed that deterrence in cyberspace is not really operational at the strategic level of conflict. They based their judgements in part on the ability of air-gapped systems to re resistant to cyber attack without insider help and on the ability to defeat cyber attacks with good planning. They did analyse the idea of "perfect cyber storm", by reference to the book *Cyber War* (Clarke and Knake 2010), but Sommers and Brown found several reasons why that sort of scenario was implausible or at least very difficult to construct (46).

In 2012, Thomas Rid published his equally seminal article, "Cyber War Will Not Take Place", followed by his book of the same title a year later (Rid 2013). It is not difficult to agree with his primary thesis: "cyber war" independent of the non-cyber domain is probably unimaginable since war of any kind is an act involving the political, economic and civilian resources of states, as well as their military technological resources, both non-kinetic (including cyber) and kinetic (including bombs and missiles). The Rid thesis was often misinterpreted to mean that a war premised on dominance in ICT and cyber warfare was some sort of exaggeration. Several studies, for example Libicki (2012), pushed the line that cyber weapons could not achieve strategic level outcomes in war.

But the scholarship about the importance of studying cyber-enable war remained vibrant, and a heavy focus of some of this work was CIIP. For example, in 2012, the *National Cyber Security Framework Manual* observes that governments "recognise that a disruption in one infrastructure can easily propagate into other infrastructures" with catastrophic consequences (Hathaway and Klimburg 2012: 36). It also observes that highly developed resilience strategies for extreme cyber emergencies are an essential part of military deterrence in the cyber age (Klimburg and Healey 2012: 84-86).

Lewis (2014) offers an essential text book for the study of risk analysis and vulnerability in critical infrastructure and key systems (CIKR), with heavy emphasis on cyber aspects. It is comprehensive and encyclopaedic in scope. It grew out of efforts sponsored by the U.S. Department of Homeland Security after 2001 to develop a curriculum in critical infrastructure protection, with the first edition being published in 2006. Its basic orientation is the relationship between policy and technology, illustrated in the Preface by the suggestion that the book offers policy makers tools to frame their decision-making: "Does changing a regulation reduce spectral radius? Does hardening of one asset make others more likely to fail?" The book contains "practical questions asked by fire protection, law enforcement, public administration, urban planning, criminology, political science, and homeland security practitioners". The book has 17 chapters in three parts: Origins of Homeland Security and Critical Infrastructure Protection Policy; Theory and Foundations (3 chapters); Individual Sectors (13 chapters). It has "five appendices containing supplemental material on probability, risk, spectral radius, tragedy of the commons, and a glossary of terms—for the extra-curious and mathematically prepared reader." At the same time, the book *d*oes not examine cyber civil defence as a policy objective, nor does not address broader social and political aspects of cyber civil defence. It analyses threat more form the vulnerability perspective than from the point of view of threat actors.

Niglia (2016 ed.) is a first-class study based on contributions from a range of scholars from NATO countries who have collectively provided important insights on leading topics of

critical infrastructure protection from a variety of sources. There are higher level policy studies (NATO's collective response, a possible role for OSCE, dialogue with industry), sector-based sturdies (such as Ports), threat-based studies (Da'esh, Russia), concept development (resilience), country studies (Ukraine, Sweden), a technical cyber attack vector analysis (firmware), and considerable attention to social media and political influencing. The book, based on a NATO Advanced Research Workshop, addresses threats from several sources, including cyber attack, information warfare, natural disaster, and maritime security. It has a heavy focus on lower level operational aspects of cyber civil defence. The one chapter that comes closest to the aim of this paper is "Sweden Under Attack!" Lessons from Past Incidents for Coping with a Comprehensive Synchronized Attack on Critical Energy and Information Infrastructure".

Kello (2016) article sets up the problem from one key perspective: "the possible strategic and other consequences of arming the civilian quarters of cyberspace with active defense capabilities". His article is premised on the globally accepted reality that states cannot adequately protect their private corporations, including critical infrastructure, in cyber space.

In a literature review on the impact of dependencies on CIIP, Thakur (2016) confirmed a very low level of engagement by scholars, outside of three U.S. based-research centres, in the policy dynamics of cyber civil defence for extreme contingencies. These centres were the Idaho National Laboratory (INL), the Argonne National Laboratory, and Carnegie Mellon University (CMU). In a 2016 study from CMU, the authors observed that one of the top priorities for regulators is managing operational risk profiles in situations "when both the management and status of key external dependencies is uncertain" (Carnegie Mellon 2016:5).

In a 46-page monograph, James Lewis (2018) correctly assesses the main source of threat for large scale debilitating cyber attacks (the cyber storm) as states rather than criminals or terrorists. The book is an important corrective to earlier studies which were not inclined to see states as the main source of such threats, though Sommers and Brown (2011) did so. At the same time, the report concentrates on the likelihood of such an attack and sees it as low, a view widely shared. But in playing down the likelihood, Lewis also appears to play down the importance of contingency planning for such an event. The work does not analyse in any depth the appropriate response of states. It is normal for states, especially in the West, to have contingency plans for highly unlikely events, including for example nuclear war, mass terrorist events, or large-scale natural disasters. The report has understated the global impact of several significant cyber attacks, especially the theft and subsequent release by Russian hackers of a small trove of U.S. cyber weapons (malware).

Cyber Civil Defence Gaps: Filling Them

The above analysis, and other work by the author, allows us to identify several important gaps in national preparedness for extreme cyber emergencies in almost all countries. The list, set out in Table 2, is a long one. It also includes, without elaboration in this paper, recommendations for actions that might be undertaken to fill the gaps

Table 2: List of Cyber Civil Defence Mini-Gaps

Gap	Fill it with:
Imagination gap	Have a (detailed) futuristic vision of cyber storm
Planning and documentation gap	Formalise comprehensive policy and publish a doctrine
Mobilisation gap	Crisis preparedness with public participation

Civil military gap	Set up a Cyber Civil Corps, led by a military officer
Private/public planning gap	Set up a multi-stakeholder National Resilience Task Force
Decision-making technologies gap	Elevate resilience spend by 500/1000 per cent
Techno-social gap	Institute cyber ecosystem planning
Interdependencies knowledge gap	Set up a dedicated national research centre
Information sharing gap	Frame protocols for sensitive information sharing
Communications protocol gap	Establish dedicated nation-wide channels and formats
Situational awareness gap	Build a "high performance" complex system
Trust gap	Build the highest quality cyber civil defence system
Legal gap	Pass new and dedicated cyber civil defence law
Open source/secrecy gap	Declassify what the "enemies" already know
Education gap	Set up a joint public/private National Cyber War College
Research gap	Fund at least one cyber civil defence research centre
Training gap	Formalise cyber civil defence training countrywide
Exercise gap	Plan annual nationwide exercises for senior executives
Evaluation gap	Commission formal 3-year evaluations

This is a huge policy agenda. In most countries it has been subordinated to the urgency of setting in place or updating basic cyber security strategies, a challenge that has been exacerbated by constantly escalating threats and low budget allocations in most sectors. Those national jurisdictions that have moved on cyber civil defence have put in place some foundation stones, but these may wait a decade or more to see an edifice of mature cyber civil defence take form. This is especially the case in federal systems of governments where law enforcement and emergency response rests with sub-national governments.

The policy agenda proposed in Table 2 raises questions about sequencing (prioritisation) and budget allocations. Many of the measures may be beyond all but a small number of developed countries, but could perhaps be handled quite comfortably by some international collaborative arrangements. For example, one could imagine an ASEAN PLUS Cyber Defence College or a BRICS equivalent.

Table 2 offers little insight into how the measures might be implement and who should lead. It has become quite clear that none of the four main actor sets (government, military, private sector or universities) can rise to any of the challenges by acting in isolation. Moreover, experience globally shows that any of these actors, if left to themselves, tend to move slowly and incrementally. The problem set almost certainly needs need new energy, new vision and a new paradigm. Change will need to be driven through a new institutional centre of gravity that is multi-stakeholder. Such a focal point is essential, and will probably need to take the form of a joint military/civilian National Information Warfare College or National Cyber Civil Corps College, as I have previously suggested for Australia (Austin 2017: 19).

The DHS ten-point CRR provides a clear pathway for evaluating the quality of a national CIIP system. As one illustration, building off the discussion above, one might look at what could usefully be done in Australia as priority measures, including:

- A cyber civil defence policy and system for CIIP
- A situational awareness system for monitoring dependencies in government and the private sector; and communicating threats and vulnerability assessments at allow level of security classification and bearing in mind that the enemies already know what we are we should be hiding
- Private enterprise response groups and plans by sector (e.g. financial services)
- Regular executive level exercises, at national and key locality levels

- Documentation of plans and procedures for benefit of all stakeholders
- the first public domain mapping of Australia's civil cyber space reality at national, state and local levels
- the first public domain mapping for assessing critical cyber interdependencies in national infrastructure
- the first National Cyber Resilience Blueprint specific to Australia, as recommended by Scully (2014)
- metrics for resilience of critical infrastructure cyber systems
- new technologies for mitigation of cyber effects and associated non-cyber risks
- responses for community level (localized) cyber-space effects of national-level cyber disruptions
- mitigation of impacts of mobile and distributed computing on national resilience
- a new paradigm of adaptability for resilience to extreme cyber space contingencies.

Conclusions and Further Research Questions

One year before Russian attacks on Estonia in 2007 brought key elements of national infrastructure in the small country to a standstill for up to two weeks, the United States and at least one ally had begun exercising for a "Cyber Storm". But in subsequent exercises in that series, the Estonian experience informed a heavier reliance on a scenario of mass attack on critical infrastructure by an adversary seeking political or economic gain. An implicit assumption of these exercises was that such an attack was taking place below the level of armed conflict as understood in international law and in the relative calm of peacetime. By 2019, the policy intensity of military planning in a few countries for such attacks (or defence against them) had reached a certain fever pitch. In 2015, China declared cyber space, along with outer space, as the "commanding heights of all international security competition". The United States announced in 2015 that it may be lawful in wartime to attack the civil nuclear power stations or dams of an enemy, leaving unsaid that the safest way to do so would be by cyber means. But the most influential event of all was Russia's escalation in January 2016 of hybrid information warfare against the United States and the European Union to weaken them without provoking war. Russia had waged a similar style of war on Ukraine since 2014, including through use of attacks on critical infrastructure, not to mention a direct armed insurgency. In 2017, President Trump declared a cyber arms race. In the process, his Administration redefined peace as if it meant simply a continuation of warfare by other means without provoking a military response, not the binary opposite of war. In 2018, Britain revealed publicly that it was prepared to black out Moscow using cyber attack if there was crisis that warranted it. By 2019, these more recent events suggest that as we look to the future, it is probably more appropriate to think about cyber blitzkrieg.

With this evolution very much at the centre of their thinking, an increasing number of states now accept that cyber civil defence is not only a necessity, but also that it is achievable. Yet few countries have set in place the mechanisms to implement cyber civil defence, let alone provide their citizens, stakeholders and partners with a narrative that can explain the difficulties and complexity of the task.

This circumstance can be interpreted to mean that there is today and prospectively a cyber civil defence gap that is now in play in international affairs in such a way as to strengthen the strategic hand of those who are better prepared, such as the United States, than those that less prepared (almost every other country).

The paper identified 19 elements of the civil defence gap (so-called “mini-gaps”) that can be seen in the security posture of most countries that would need to be addressed in some strategic and unique combination to begin to nullify the consequences of such gaps. While this is a demanding policy agenda, it carries with it–for countries committed to evidence-based policy or even basic knowledge– the implication that it is also a demanding research agenda. Both challenges (filling policy gaps and undertaking comprehensive research) can be addressed in one hit by creating new knowledge communities that also service the policy demands. An example of this would be the creation of a Cyber Civil Defence College at national level, perhaps associated with establishment of a Cyber Civil Defence Corps, as this author has suggested for Australian. By such a move, a government could hope to relieve itself of the day to day burden of policy development and national mobilisation for cyber civil defence. Such institutions could also be created on a multinational level among allied or friendly states to share costs and marshal talented personnel.

Future cyber civil defence will need to pay far more attention to the psychological warfare element of the problem to complement reasonably well-developed understanding of the sabotage element (cyber attack). This latter element has by itself dominated almost all studies on CIIP so far. New policy will need to assume that defence of CIIP in the future will be made far more difficult because of the ubiquity of information infrastructure, with the Internet of Things becoming as much a target as so-called critical assets identified by sector (such as power, water, transport). In fact, the protection of the internet itself, a uniquely international, critical infrastructure should be a high priority for cyber civil defence at the national level.

Even as the confrontations between pairs of countries or whole alliances are intensifying, there will need to be new international cooperative activity that seems to fly in the face of deepening alliance cohesion. New analytical approaches will be mandatory, including comprehensive investigation of social and political aspects of cyber civil defence. Countries that continue to privilege technical cyber security specialists over other professionals in cyber civil defence will falter.

An orientation toward specific threat actors, as advocated by James Lewis, rather than an apolitical orientation toward technical vulnerabilities in systems, will also be essential. A fundamental ingredient of national cyber civil defence capability will be access to advanced simulations of extreme cyber events as they may play out differently in each country, and even in key localities (such as major cities). Where countries and organisations do not have this capability, they should set up the necessary national and international relationships to access it regularly and on a consistently high-quality basis.

All states, including the most powerful, are facing a contested, catch-up in cyber civil defence in which paradigm-changing decisions about priorities, reform strategies, budgets and international alliances seem inescapable.

REFERENCES

AEMO. 2017. Black System South Australia. Australian Electricity Market Operator. https://www.aemo.com.au/-/media/Files/Electricity/NEM/Market_Notices_and_Events/Power_System_Incident_Reports/2017/Integrated-Final-Report-SA-Black-System-28-September-2016.pdf

Arce D.G. 2015. WikiLeaks and the risks to critical foreign dependencies. *International Journal of Critical Infrastructure Protection* 2015 (11) December 3-11

Austin G. 2016. Australia Rearmed. Future Needs for Cyber-Enabled Warfare. ACCS Discussion Paper #1. University of New South Wales Canberra. https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/Discussion%20Paper%20%231.pdf

Austin G. 2017. Human Capital for Cyber Security: The Australian Case. ACCS Briefing Paper #2. University of New South Wales Canberra. https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/Briefing%20Paper%232%20Human%20Capital%20for%20Cyber%20Security%20Web.pdf

Austin G. 2018a. Keeping up with the Pentagon in the Information Age. ASPI Strategist. 3 September 2018. https://www.aspistrategist.org.au/keeping-up-with-the-pentagon-in-the-information-age/

Austin G. 2018b. *Cybersecurity in China*. Springer International

Austin G. and Sharikov P. 2016. Pre-emption is victory": aggravated nuclear instability of the information age. *The Nonproliferation Review 23*(5-6) 691-704

Baumard P. 2017. *Cybersecurity in France*. Springer International Publishing

Clarke R.A. and Knake R.K. 2014. *Cyber war*. Tantor Media Incorporated

CMU. 2016. External Dependencies Management, Carnegie Mellon University, in cooperation with U.S. CERT. https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-EDM.pdf. Accessed 14 January 2018.

DCI. 1978. SOVIET CIVIL DEFENSE (NI 78-10003). Director of Central Intelligence. http://www.faqs.org/cia/docs/44/0000500560/SOVIET-CIVIL-DEFENSE-(NI-78-10003).html#ixzz5blqDmnK6

Deloitte and NASCIO. 2018. 2018 Deloitte-NASCIO Cybersecurity Study. States at risk: Bold plays for change. A Joint Report from Deloitte and the National Association of State Chief Information Officers (NASCIO).

DHS. 2006. Civil Defense and Homeland Security: A Short History of National Preparedness Efforts. Homeland Defense National Preparedness Task Force. https://training.fema.gov/hiedu/docs/dhs%20civil%20defense-hs%20-%20short%20history.pdf

DHS. 2008. Fact Sheet: Critical Infrastructure and Homeland Security Protection Accomplishments. Department of Homeland Security, 5 September 2008. https://www.hsdl.org/?abstract&did=235174

DHS. 2009. Cyber Resilience Review. Department of Homeland Security. https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf

DHS. 2011. PPD8: National Preparedness. https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

DHS. 2018a. Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure

DoD. 2018. Strategy. Joint Doctrine Note 1-18. https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_18.pdf?ver=2018-04-25-150439-540

Dudenhoeffer D.D. Permann M.R. and Manic M. 2006. CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. In Perrone, L.F., Wieland, F.P., Liu, J., Lawson, B.G., Nicol, D.M. and Fujimoto, R.M. (eds.) Proceedings of the 2006 Winter Simulation Conference. 478-485 https://www.researchgate.net/profile/Milos_Manic/publication/221527820_CIMS_A_Framework_for_Infrastructure_Interdependency_Modeling_and_Analysis/links/547608080cf2778985b0791a.pdf

Frieser, KH. 2013. *The Blitzkrieg Legend*. Naval Institute Press. Translation from the German first edition of 1966

G8. 2003. Principles for the Protection of Critical Information Infrastructures. May 2003. http://cybersecuritycooperation.org/documents/G8_CIIP_Principles.pdf

Gady F. and Austin G. 2010. Russia, the United States, and Cyber Diplomacy: Opening the Doors. EastWest Institute. New York/Brussels/Moscow. 20pp. https://www.eastwest.ngo/sites/default/files/ideas-files/USRussiaCyber_WEB.pdf

Garrison D. 2006. *Bracing for Armageddon: Why civil defense never worked*. Oxford University Press

Hansen L. and Nissenbaum H. 2009. Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly 53*(4) 1155-1175

Hart Rudmann. 2001. Road Map for National Security: Imperative for Change. The Phase III Report of the U.S. Commission on National Security/21st Century. The United States Commission on National Security/21st Century. 15 February 2001. http://www.au.af.mil/au/awc/awcgate/nssg/phaseIIIfr.pdf

Hathaway M.E. and Klimburg A. 2012. Preliminary Considerations: On National Cyber Security. In Klimburg A. ed. 2012. *National cyber security framework manual*. NATO Cooperative Cyber Defense Center of Excellence. 1-43. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

INL Website. 2016. Grand Challenge in Resilient Control Systems. https://icis.inl.gov/SitePages/Grand%20Challenge%20in%20Resilient%20Control%20Systems.aspx. Accessed 30 June 2016.

INL Website. Idaho National Laboratory. Grand Challenge in Resilient Control Systems. https://icis.inl.gov/SitePages/Grand%20Challenge%20in%20Resilient%20Control%20Systems.aspx. Accessed 12 January 2019.

Insurance Journal. 2018. Most Global Organizations Fail to Lear from Cyber Mistakes: WTW Survey. Accessed 13 January 2019.

JCS. 2018 b. Homeland Defense. JP 3-27. Joint Chiefs of Staff. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_27.pdf?ver=2018-07-09-162710-440

JCS. 2018a. Cyberspace Operations. JP 3-12. Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150

Joint Committee. 2018. House of Lords and House of Commons Joint Committee on the National Security Strategy Cyber Security of the UK's Critical National Infrastructure Third Report of Session 2017–19. 19 November 2018.

Keliiaa C.M. and Hamlet J.R. 2010. National Cyber Defense High Performance Computing and Analysis: Concepts, Planning and Roadmap. SANDIA Report SAND2010-4766. pp.7-8. http://prod.sandia.gov/techlib/access-control.cgi/2010/104766.pdf. Accessed 30 June 2016.

Kello, L. 2016. Private-Sector Cyberweapons: Strategic and Other Consequences. 15 June 2016. Available at SSRN: https://ssrn.com/abstract=2836196 or http://dx.doi.org/10.2139/ssrn.2836196

Klimburg A. and Healey J. 2012. Strategic Goals and Stakeholders. In Klimburg A. ed. 2012. *National cyber security framework manual*. NATO Cooperative Cyber Defense Center of Excellence. 66-107. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

Lewis J. 2018. *Rethinking Cybersecurity: Strategy, Mass Effect, and States*. CSIS. 46pp

Lewis T.G. 2014. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. John Wiley & Sons. 367 pp

NIAC. 2017. Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure. The President's National Infrastructure Advisory Council. https://www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf

Niglia A. (ed) 2016. Critical Infrastructure Protection Against Hybrid Warfare Security Related Challenges. IOS Press in cooperation with the NATO Emerging Security Threats Division. 157pp

Pescaroli G. and Kelman I. 2017. How critical infrastructure orients international relief in cascading disasters. *Journal of Contingencies and Crisis Management 25*(2) 56-67

Posen B. 1984. *The Sources of Military Doctrine*. Ithaca NY. Cornell University Press

Purdy A. 2005. Prepared Statement. Joint Hearing before the subcommittee on Economic Security, Infrastructure Protection, and Cybersecurity with the Subcommittee on Emergency Preparedness, Science, and Technology of the Committee on Homeland Security. House of Representatives 109th Congress. First Session. 18 October 2005. p9. https://pdfs.semanticscholar.org/8624/d5dcb8b964b03461bfc3f738faf392cb8927.pdf

Rauscher K.F. Krock R.E. and Runyon J.P. 2006. Eight ingredients of communications infrastructure: A systematic and comprehensive framework for enhancing network reliability and security. *Bell Labs Technical Journal* 11.3 73-81

Rid T. 2012. Cyber War Will Not Take Place. *Journal of Strategic Studies*. 35:1 5-32. DOI: 10.1080/01402390.2011.608939

Rid T. 2013. Cyber War Will Not Take Place. London. Hurst Publishing.

Scully T. 2014. Defence White Paper 2015 Submission. A National Cyber Resilience Blueprint. http://www.defence.gov.au/Whitepaper/docs/142-Scully.pdf

Sharma M. 2019. "India and China: Ignoring the Storm Warnings", paper prepared for the International Conference on Research and Education for the Cyber Storm, February 2019, University of New south Wales Canberra

Slayton R. 2017. What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security 41*(3) 72-109

Snyder J. 1985. *The Ideology of the Offensive*. Ithaca NY. Cornell University Press

Sommer P. and Brown I. 2011. Reducing Systemic Cybersecurity Risk. OECD. FP/WKP/FGS (2011)3

Stacey B. 2015. Statement of Mr. Brent J. Stacey, Associate Laboratory Director National & Homeland Security Idaho National Laboratory before the United States House of Representatives Science Subcommittee on Energy and Science Subcommittee on Research and Technology, 21 October 2015

Tabansky L. and ben Israel I. 2015. Cybersecurity in Israel. Springer International

Tehan D. 2016. Address to the National Press Club. A Cyber Storm. 23 November 2016. https://ministers.pmc.gov.au/tehan/2016/address-national-press-club-cyber-storm

Thakur M. 2016. Cyber Dependency at a National and International Level. A Literature Review. Australian Centre for Cyber Security

UNGA. 2015. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174. 22 July 2015. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

United Nations Treaties. 1979. First Additional Protocol to the Geneva Conventions of 1949. https://treaties.un.org/doc/Publication/UNTS/Volume%201125/volume-1125-I-17512-English.pdf. Accessed 15 January 2019.

Vale L.J. 1987. *The limits of civil defence in the USA, Switzerland, Britain and the Soviet Union: the evolution of policies since 1945*. Springer

White House. 2016. PPD 41, President Policy Directive: United States Cyber Incident Coordination, July 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

White House. 2017a. Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. 11 May 11, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

White House. 2017b. National Security Strategy of the United States of America. December 2017. http://nssarchive.us/wp-content/uploads/2017/12/2017.pdf

Xinhua. 2014. January 7, 2014 http://news.xinhuanet.com/mil/2014-01/07/c_125948370.htm accessed 1 February 2014. This webpage is no longer available.

Author Note

Greg Austin is a Professor in the UNSW Canberra Cyber. He concurrently serves as a Professorial Fellow with the EastWest Institute (EWI), with offices in New York, Palo Alto, Brussels and Moscow. He is Australia's leading research scholar on international security aspects of cyber space affairs. He coordinates a Research Group on Cyber War and Peace at UNSW and leads international research projects on cyber security policy. He set up Australia's first Master's degree in Cyber Security, Strategy and Diplomacy (which has few peers anywhere in the world), and teaches four subjects in this degree. Greg is a member of the Cyber Security Advisory Council for the Australian state of New South Wales and a member of the Advisory Board for the Global Foundation for Cyber Studies and Research, registered in the United States. He has published two books on cyber policy on China (2014 and 2018), one of a tiny group of scholars to do so. His other publications include five books on Asian security affairs (four are on China), each with a strong interdisciplinary focus, and one additional edited volume on energy security. His research interests concentrate on cyber strategy and diplomacy, security policies of China and Russia, countering violent extremism, and national security ethics. He has held seven university appointments, all in world class universities or departments: War Studies at King's College (Senior Visiting Fellow), Peace Studies at Bradford (Associate Professor), International Relations at ANU in Australia (Fellow). He has held posts in Australian security policy as Ministerial adviser, parliamentary committee secretary, international intelligence liaison officer, and intelligence analyst. He is a member of the Cyber Security Advisory Council of the New South Wales state government.

Selected Scholarly Publications by Greg Austin

Books

Cyber Security in China, Springer, 2018
Cyber Policy in China, Polity Press, Cambridge, 2014

Books in Progress

(ed.) *Civil Defence Gaps for the Cyber Storm* (in progress)
(ed. with Tom Sear) *Human Capital for Security in Cyberspace* (in progress)

Journal Articles/Book Chapters/Policy Reports

Policy Dilemmas in Cyber Security Human Capital Formation. In Austin G and Sear T (eds.) *Human Capital for Security in Cyberspace* (forthcoming)

Opportunity, Threat and Dependency in the Social Infosphere. in Cornish P (ed.) *Oxford Handbook on Cyber Security.* Oxford University Press, Oxford. forthcoming

Global Trade and Cyber Security: Monitoring, Enforcement and Sanctions. Co-authored with Gady FS in Cornish P (ed.) *Oxford Handbook of Cyber Security*, Oxford University Press. Oxford. forthcoming

Preemption Is Victory: Aggravated Nuclear Instability of the Information Age. 2017. co-authored with Pavel Sharikov, Russian Academy of Social Sciences. *Non-proliferation Review* 23 (5-6) 691-704

Robots Writing Chinese and Fighting Underwater. 2017. in Kiggins R. (ed.) *The Political Economy of Robots: Prospects for Peace and Prosperity in the Automated 21st Century*. Palgrave. 271-290

Restraint and Governance in Cyberspace. 2017. in Burke A and Parker R (eds.) *Global Insecurity: Futures of Chaos and Governance*. Palgrave. 215-233

Are Australia's responses to cyber security adequate?. 2017. *Australia's Place in the World.* CEDA. 50-61. http://www.ceda.com.au/Research-and-policy/All-CEDA-research/Research-catalogue/Australia-s-place-in-the-world

Middle Powers and Cyber-Enabled Warfare: The Imperative of Collective Security. 2016. in Munish Sharma and Cherian Samuel (eds). *Securing Cyberspace: Asia and International Perspectives.* IDSA. Pentagon Press. New Delhi. 23-56

International Legal Norms in Cyberspace: Evolution of China's National Security Motivations. 2016. in Anna-Maria Osula and Henry Rõigas (eds). *International Cyber Norms: Legal, Policy & Industry Perspectives.* NATO CCDCOE Publications. Tallinn. 172-201

Australia's Response to Advanced Technology Threats: An Agenda for the Next Government. 2016. co-authored with Jill Slay. Australian Centre for Cyber Security. Discussion Paper #3. University of New South Wales Canberra

Australia Rearmed: Future Needs for Cyber-enabled War. 2016. Australian Centre for Cyber Security, Discussion Paper #1. University of New South Wales Canberra

Promoting International Cyber Norms: A New Advocacy Forum. 2015. co-authored with Bruce McConnell and Jan Neutze. EastWest Institute. New York/Brussels/Moscow. 19pp

China's Security in the Information Age. 2015. L. Dittmer and M. Yu (eds). *Routledge Handbook of Chinese Security.* Routledge. 355-370

China's Cyber Espionage: The National Security Distinction and U.S. Diplomacy. 2015. Discussion paper. 9,000 words. Available at http://thediplomat.com/wp-content/uploads/2015/05/thediplomat_2015-05-21_22-14-05.pdf

Australia's Digital Skills for Peace and War. 2014. *Australian Journal of Telecommunications and the Digital Economy* 2 (4) 68:1-15

Managing Asymmetries in Chinese and American Cyber Power. 2014. *Georgetown Journal of International Affairs.* International Engagement on Cyber IV. 141-151

Australian Defence Policy in the Information Age. Submission for the 2015 Australian Defence White Paper. 22 September 2014. 5,000 words. http://www.defence.gov.au/Whitepaper/docs/028-Austin.pdf

A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets. 2014. co- authored with Eric Cappon, Bruce McConnell, Nadia Kostyuk. EastWest Institute. New York/Brussels/Moscow. 26pp

Resetting the System: Why Highly Secure Computing Should Be the Priority of Cybersecurity Policies. 2014. co-authored with Sandro Gaycken. EastWest Institute, New York/Brussels/Moscow.

Cyber Detente between the United States and China. 2012. co-authored with Franz Stefan Gady. EastWest Institute. New York/Brussels/Moscow. 20pp

Russia, the United States, and Cyber Diplomacy: Opening the Doors. 2010. co-authored with Franz Stefan Gady. EastWest Institute. New York/Brussels/Moscow. 20pp

Recent News Commentaries

Should cyber officials be required to tell victims of cyber crimes they've been hacked. The Conversation. January 2019

New guidelines for responding to cyber attacks don't go far enough. The Conversation. 18 December 2018

Keeping up with the Pentagon in the Information Age. ASPI Strategist. 3 September 2018

Explaining Australia's Sharp Turn to Information Warfare. *The Diplomat*. 8 July 2017

'Cyber revolution' in Australian Defence Force demands rethink of staff, training and policy. The Conversation. 4 July 2017