Shifting the Boundaries: Conceptual and Practical Challenges of Cybersecurity Education, Definitions and Expectations

Sean S. Costigan

A commentary submitted in partial fulfilment

of the requirements for the degree of Doctor of Philosophy by publication

(Criminology)

at the

University of Portsmouth

January 2023

Table of Contents

Acknowledgements

Writing a commentary on the value and merit of one's academic contributions and publications is a novel and clarifying wisdom exercise in which few scholars may engage. In hindsight, writing such a commentary during a (hopefully) once in a lifetime pandemic may appear to be apt timing. If I have been able to see a little further, it is thanks to the shoulders of my relatives, dear friends and colleagues. I wish to thank my parents, John and Christina Costigan, and my uncle Joseph Sarkissian and aunt Helen Kourtjian, for instilling the value of education as a pursuit in itself and my wife for supporting my pursuits and challenging my thinking. My many learned colleagues have shown the virtues of humility and service, which I seek to emulate, and have gently prodded and guided me. In particular, I would like to thank Dr. David Bray, Ms. Jeannie Callaghan, Dr. Paul Erickson, Dr. Kenneth Estes, LTC Olaf Garlich, Dr. Greg Gleason, Dr. Namrata Goswami, Dr. Michael Hennessy, Dr. Graeme Herd, Dr. Kenneth Keller, Dr. Dinos Kerigan-Kyrou, Mr. Frederic Labarre, Dr. Scott Knight, COL (ret) Phil Lark, Dr. Gustav Lindstrom, Dr. Ann Markusen, CDR Jonathan Odom, Mr. Chris Pallaris, Mr. Jake Perry, Dr. Detlef Puhl, Dr. John Schindler, Dr. Everita Silina, Dr. Al Stolberg, Dr. Todor Tagarev, and Mr. Max Wolff, among others. I also wish to thank my august examiners, Dr. Sylvain Leblanc, Dr. Lisa Sugiura, and Dr. Alison Wakefield. I am deeply indebted to my academic supervisors at the University of Portsmouth, Dr. Vasileios Karagiannopoulos and Dr. Mike Nash, for having graciously taken me on as a student and sharpened my thinking and awareness of pathways for future scholarship. Finally, I would like to thank my students without whom I would not have been able to test the merit of ideas and, humbly, to experiment, learn, and strive for better.

I. Introduction

‘A talent for following the ways of yesterday is not sufficient to improve the world of today.’ King Wu-ling, 307 BC

The aim of this commentary is to develop an integrated understanding of my original contributions and approaches to assessing international security institutions’ challenges and capacities to manage disruptive change, particularly through case studies of historical and contemporary need for cybersecurity awareness and education. This commentary specifies and contextualises my contributions to scholarship and research in cybersecurity, emerging security challenges and security education. In particular, emphasis is paid to the roles that defence institutions and national defence policymakers play as intellectual and resource gatekeepers. Biases are also explored at length, particularly those that may affect authoritative responses, mitigate surprise, or allow for improved anticipation and resilience.

The organisation of this commentary is in six parts. Following this introduction, I situate my publications in wider scholarship, synthesise them to detail conceptual frameworks and assumptions, and elucidate my original contributions and frameworks on emerging security challenges and cybersecurity. Two central questions are addressed in this commentary:

1. In what ways have international security institutions come to understand and account for change in cybersecurity?

2. How do institutional cultures and biases hinder responses to emerging technological issues and security educational efforts; and what might be done?

Throughout the commentary, I contextualise the creation and intellectual contribution of my publications and specify their domain boundaries, ending with a conclusion that offers proposals for improvements for cybersecurity education. Perforce this is a selective review and so it would seem wise at the outset to make note of my partiality for foresight techniques and, in particular, examinations of past and present weak signals and what they may portend for societal and institutional readiness in times of change.

Principally, my research and publications detail these challenges and provide potential remedies or areas for further study. In other cases, the issues I note in my publications emerge from subsequent fieldwork or the reception of my publications. In both cases, my publications provide original frameworks for conceptualisation and confer opportunities to operationalise theories, putting cybersecurity concerns into practice through pedagogic and policy works. My research is an expansion of my scholarly journey as an academic and practitioner, developing multidisciplinary approaches to improve security and education and redress imbalances in cybersecurity postures. Taken as a whole, I firmly believe that the diversity, quality, and impact of my work is at the doctoral level.

As a student of history, practitioner and educator of international security, and a technologist, I note that, in my experience, paradigmatic change and related

epistemic issues are often only slowly recognized by authorities. This challenge is accentuated and made more acute in international institutions that carry the mantle of security and defence.[1] My published works highlight clearly defined indicators of impediments at security institutions and in their conceptualisations of new risk. The identification of new risk and related blockages, as well as the potential for remedies, is in fact a continuous theme in my work, starting in early publications such as my 2007 study 'Terrorists and the Internet: Crashing or Cashing In?' or my 2009 U.S. intelligence community work which developed new models for understanding non-traditional challenges and led, among other outcomes, to the publication of 'Cultivating Strategic Foresight for Energy and Environmental Security'. In these, and other works, I detail the cognitive and institutional impediments that may produce insecurity or, put differently, allow people and their governments to remain underprepared for change.

The analytical process of first noting technological change and then examining potential security concerns and institutional impediments to inform education and policy continues in my work through today. The same thread is woven through my journal articles (Costigan & Gleason, 2019; Costigan & Lindstrom, 2016) policy essays and reports (Bray et al., 2009; Herd et al., 2013), book chapters and books, for instance *Cyberspaces and Global Affairs* (Costigan & Perry, 2016), 'Cybersecurity, Global Governance and New Risk' (Costigan, 2016a), the NATO *Cybersecurity: A Generic Reference Curriculum* (Costigan & Hennessy, 2016), among others included in this commentary.

[1]For the purposes of this commentary, international security institutions are those that expressly work across national boundaries in furtherance of reducing or addressing potential security threats.

The doctoral-level publications described in this commentary include four distinct types:

1. Academic investigations into how international security institutions come to understand and engage with emerging technologies, particularly transformative changes in cybersecurity.
2. Practitioner publications that present pedagogical openings to improve results in intractable cybersecurity problems.
3. Policy publications that contribute original understanding of how academic or theoretical works may come to be operationalised in international security institutions.
4. Related field investigations and presentations are also included where these have produced new insights that emerge from teaching or using my publications.

Professionally, my perspectives are deeply informed by my education in the history of science and vocational experience working for high-profile defence organisations and think tanks, such as the United States Department of Defense, the Center for Security Studies (ETH Zurich), and the Council on Foreign Relations, among others. My experience is equally informed by my inculcation, and resulting productive collaborations, in the fields of emerging security challenges and foresight. As such, a significant amount of my analytical and creative output has been produced under the rubric of government-supported or policy efforts, often with the express intention of exposing ‘gaps and seams’ in security conceptualizations, policy scholarship, or

related educational programmes. By design, the foresight and emerging security challenges publications in this commentary are forward-leaning investigations which detail future, yet still tangible and actionable, potentially high impact developments. Such studies typically seek to offer potential glimpses into multiple futures and pathways for policy and security education.

Notably, security scholars and practitioners often consign emerging security challenges and foresight to the domains of intelligence or future studies. However, as my research in cybersecurity and emerging security challenges indicates, relegating complex, paradigm-changing emergences to a single domain or profession may be fraught with societal risk (Bray et al., 2009; Costigan, 2016c, 2016a; Costigan & Lindstrom, 2016; Herd et al., 2013). For example, intelligence (thought of here as a state function to alert to security risk) is rarely shared outside of political leadership and typically remains classified. While awareness of risk may exist in classified environments, such knowledge – even when potentially accurate – may be forgotten, overlooked, or left to stagnate (Betts, 1978; Hedley, 2005). Likewise, while an academic domain such as media studies may be engaged in research into changing technologies, little transdisciplinary work is done between security researchers, media scholars, and engineering professionals (Althonayan & Andronache, 2018; Blair et al., 2019; Vishik & Balduccini, 2015). My work seeks to address these imbalances and offers remedies to further the timely sharing and co-creation of knowledge, among other proposed solutions (Bray et al., 2009; Costigan, 2016a).

II. Framing the Scholarship and Publications

Since the start of the information age, developments in information and communication technologies have regularly yielded surprises for domestic and international security institutions. Imagination, the 'sine qua non of creativity' (Stuart, 2022), appears to have been deficient while failures of imagination have cost society and their governments dearly (Kean et al., 2004; Weick, 2005, 2006). Often these failures are noted and felt most acutely in times of volatile world events and in areas of paradigmatic technological change, which may also include a hitherto novel application of pre-existing technology. Examples of such paradigmatic changes run the gamut from the inability to imagine the use of hijacked passenger jetliners qua missiles (as in the world-changing events of 9/11) to the horrors of the world witnessing the live-streaming of a terrorist's shooting spree in Christchurch, New Zealand in 2019. For policymakers, the democratisation, pervasiveness, and vulnerabilities of information and communication technologies are now understood to have cascading, interrelated effects for states and societies.

Presently, concerns about cybersecurity have multiplied and may now be seen on many fronts (Hussain et al., 2020; Sen, 2018). To consider but one example in the 'cognitive' (human layer) of cybersecurity, policymakers and military leadership are concerned about the proliferation of alternative information sources and applications and their effects on operations (Alemanno, 2018) and scholars are studying the means to detect and deter influence operations (Alizadeh et al., 2020; Cordey, 2019). Yet cybercrime has also diversified. For example, formerly negligible ransomware activities have transformed into global and disruptive cybercrime through the adoption and novel application of emerging technologies. As in other

cases, detailed policy analysis and scholarship suggests that anticipatory efforts, educating for awareness, and knowledge sharing were not brought to bear early enough. Were such efforts put in place, it is conceivable that they might have had an appreciable impact, potentially thwarting the direst consequences.

Scholars note that security institutions often fail both to anticipate possible emerging threats and, after their emergence, may also seemingly be slow to respond (Dumaine & Mintzer, 2015; Maor, 2017; Taleb 2014). Institutions may also react hastily, among other deficits. In many cases, it appears to be the case that external factors, sometimes referred to as shocks, may be crucial to accelerate policy change or harness the intellectual nous and requisite energy for extensive, sustained institutional responses. Such shocks are often framed as 'Black Swan' events which typically reveal how ill-equipped a given society's security sector may be at predicting 'unpredictable' situations and how, in the wake of equally poor reactions to these events, proceedings may shape themselves in a way unfavourable to those most affected (Birkland, 1997; Taleb, 2007). Academics from various domains have produced exceptional scholarship on the issues of prediction and response as it relates to existential security concerns (Boyne & Entwistle, 2010; Christianson & Barton, 2021; Dumaine & Mintzer, 2015; Maor, 2017; Marsh & McConnell, 2010).

Considerable scholarly effort also has been applied to understanding how defence and security institutions come to understand and manage change (Cohen & Gooch, 2006; Mendelsohn et al., 1988) much of which finds its impetus in long-standing observations and related hypotheses – often derived through induction – on *military* failures to adopt technologies that might have proven decisive in the conduct of war

(Gouré, 2018; Hill, 2015; J. Schneider, 2019). Scholarship on wholesale technological change indicates that such change may appear as seemingly disparate ideas or developments that, when considered in hindsight, may be seen by observers as aggregations of new technologies. These aggregations emerge from progress or innovations, often as a result of academic research in scientific, industrial or even managerial domains and their eventual societal application. For example, Thomas Kuhn (whose presence loomed large in my studies at Harvard's Department of the History of Science and whose scholarship continues to inform my work) argues in *The Structure of Scientific Revolutions* that these aggregations and developments are, in fact, not linear but instead are subject to periodic revolutions (Kuhn, 1962). In the military domain, or where such aggregations may impact national and security institutions, defence academics and policymakers have conceived of an allied complex as the 'Revolution in Military Affairs' (RMA) which is defined by the United States Office of the Secretary of Defense as 'a major change…brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organisational concepts, fundamentally alters the character and conduct of military operations' (Gouré, 2018). Beginning in the late 1990s I described the shifts that high technology university and industrial research were beginning to undergo, asserting that Cold War security doctrines that had buttressed innovation and education were losing their persuasiveness which, in turn, would lead to harder to predict technological trajectories and the potential for cascading global effects (Callan et al., 1997).

While many of today's essential information technologies were created *de novo* by military or security institutions or were underwritten by them (Ceruzzi, 2003), presently many of those same institutions are confronted by rapid and disruptive change that is due in no small measure to the effects and underestimation of technological change (Costigan, 2016c; Farrell & Terriff, 2002; Lindsay, 2020; J. Schneider, 2019). Concomitantly, security institutions are taxed by heterogeneous restraints that appear to limit institutional receptiveness and the potential to respond to, or in some instances even educate for, change. Such impediments include a variety of managerial, human resource, bureaucratic, legacy, cultural, socio-technical, and conceptual challenges that limit imagination and consensus on matters of definition and doctrine, as well as the scope and scale of potential responses to change. Defence academics, policy analysts, and professional military educators may also have 'cognitive blinders' and are often focused on the 'what and how' and not the bigger question of 'why' (Bray et al., 2009; Costigan, 2016a; Herd et al., 2013).

Scholars of national security have described the defence academics employed by, or supporting, international security institutions as fitting into two camps. Put broadly, security scholars may be conceived as 'traditionalists' who argue that security is primarily about keeping a nation (or group of nations) safe from external threats, or more recently, security scholars – sometimes labelled 'futurists' – who argue for the deepening and widening of security concerns to include cybersecurity, climate change, and political or economic concerns (Anthony, 2016; Barnard-Wills & Ashenden, 2012; Dumaine & Mintzer, 2015; Solar, 2020; Vacca, 2011). Acutely, despite these differences in scholarship, in my work I noted that some emerging

security challenges may also lead to increased risks of institutional fragility or elevate the risks of planning and prioritising for the past instead of future matters (Bray et al., 2009; Costigan, 2016a; Costigan & Gleason, 2019). Long-standing research in management and policy literature on security affairs refers to these pitfalls as the preparation for the 'last war', the causes of which are multivariate (Dombrowski & Gholz, 2006; Mitroff, 1988; Mitroff et al., 1987; Rumsfeld, 2002). Avoidance of these pitfalls is of paramount importance to national defence policymakers. My work and publications demonstrate that it may be possible to bridge divides through novel conceptual frameworks, generating awareness of potential biases, and the introduction of new forms of sharing and enquiry which are explored at length in this commentary (Bray et al., 2009; Costigan, 2016a; Costigan & Pallaris, 2016; Herd et al., 2013).

III. Conceptual Frameworks for the Publications, Domain Boundaries, Development Paths, and Impacts

In some cases, international security institutions may be engaged in a discourse about how to anticipate change or, more conservatively, plan for resilience or engage in prevention from harm. In my publications introduced below and contextualised throughout this commentary, I describe some of these promising internal discourses as *knowledge ecologies* (Costigan & Pallaris, 2016; Herd et al., 2013). While these knowledge ecologies have shown promise in terms of improved sharing, research indicates that most security institutions continue long-standing traditional bureaucratic practices that tend to create and capture information and knowledge in silos, which may only nominally alter awareness and education to account for innovation (Costigan & Pallaris, 2016; Herd et al., 2013).

Despite calls for revolutionary change (Kean et al., 2004; Sylves, 2005; Walt, 1991) to create the conditions for improved awareness and greater focus on security concerns, trapped information and static education appear largely to remain the norm (Daneshmandnia, 2019; Hurel & Lobato, 2021; Mandrick & Smith, 2022; Phillips & Tanner, 2019). Information silos make it all the more unlikely that institutions will be prepared to anticipate problems, particularly surprises that may emanate from so-called 'wicked problems' which evidence 'deep interconnectedness, complexity, no clear single solution', or dilemmas related to a dynamic socio-political context (Rittel & Webber, 1974). In my publications, and for the purposes of this commentary, cybersecurity is considered a wicked problem which, for international security institutions, has pushed institutional abilities to coordinate and prioritise for change, despite not being purpose built to work on such emerging challenges, and – in so doing – has exposed institutional fragility (Costigan, 2016a; A. Hall, 2017; Head, 2022; Herd et al., 2013; Wilczek, 2021).

In keeping with that realisation, I frame an institution's internal discourse in the language of *knowledge ecologies* as a complementary approach and heir to knowledge management for security institutions. Knowledge ecologies – defined here as a vigorous and flexible discourse that takes place within a physical or virtual institution – may already be found within some international security organisations. Unlike the stovepiped systems common to knowledge management, knowledge ecologies are a reflection of emerging technological and organisational structures that are engineered to ensure resilience and flexibility in uncertainty as well as to encourage new attitudes and behaviours, especially with regard to knowledge creation and exchange. Since the advent of the web, closed and static information

systems have been confronted by calls for change as newer technologies promised openness and participation, allowing for a dialectic process of exchange (Costigan & Pallaris, 2016). The potential for these knowledge ecologies remains to extend the creation and basic accumulation of knowledge to a state of improved awareness, collaboration, learning, and adaptation. Notably, traditional processes of knowledge management and other access-based systemic approaches tend towards *optimization*, for example by providing actionable information where and when needed, but knowledge ecologies are best conceived of as aiming for context, sensemaking, and sustained community engagement (Bray et al., 2009; Costigan & Pallaris, 2016). Both formal and informal knowledge ecologies can exist within international security institutions, examples of which are further detailed in my publications and in this commentary (Costigan, 2016a; Costigan & Pallaris, 2016). Knowledge ecologies may also be reflected in institution-specific educational endeavours, to include instances in some training platforms (Bonk & Graham, 2012; Grabher, 2004; Malhotra, 2002).

Dedicated efforts to educate based on past lessons, and to maintain institutional memory, also exist in many national and international security institutions (Dyson, 2019). In military organisations, these endeavours often take the form of historical analyses, variously referred to as post-mortems or ‘lessons learned’ that then can become part of future education. Nevertheless, some research proposes that education – however delivered – is not a panacea and that lessons learned may still produce uneven results (Dyson, 2019). As security institutions operate in contested and complex environments, institutions may prefer to invest in ‘prevention’ which may be thought of here as a function of collecting sufficiently objective knowledge to

act (Massumi, 2007), instead of working towards anticipatory efforts that seek to bring about awareness and resilience for multiple futures (Costigan & Pallaris, 2016; Costigan & Perry, 2016; Dreyer & Stang, 2013; Grusin, 2010; Kaiser, 2015). In other cases noted in this commentary, waiting for change appears to be the status quo as may be the institutional tendency to overcompensate after massive external shocks (Birkland, 1997; Taleb, 2007). My publications and work offer methods for policymakers to more rapidly ascertain likely security risks and, potentially, understand the unintended consequences of disruptive technological developments that portend societal impact (Costigan, 2016a, 2016c; Costigan & Lindstrom, 2016; Costigan & Pallaris, 2016; Herd et al., 2013).

'Disruptive' or 'transformative innovation' are concepts that were first coined in graduate schools of business and are still most commonly discussed in industry and only rarely in security institutions. Yet, as noted, there is a rich history of the security institutions underestimating the complex ramifications that may result from technological or scientific advances (Christensen et al., 2013; Dombrowski & Gholz, 2009; Si & Chen, 2020). Indeed, only after external shocks do many security organisations come to consider cultural, socio-technical, or bureaucratic factors that may hamper receptiveness to innovation and concomitant risks or their crucial role in understanding and acting (Costigan, 2016c, 2016a; Costigan & Gleason, 2019). For example, after the terrorist attacks of 9/11 and the subsequent forensic analysis of that revealed compound systems failures, the security community in the United States was broadly warned by political leadership to change its longstanding practices of siloing knowledge as a first step to correct for insecurity (Kean et al., 2004). To put that political instruction into the language summarising the major

cultural shift of the time: security institutions were told to move from ‘need to know’ to ‘need to share’ (Bray et al., 2009; Costigan, 2016a; Dawes et al., 2009). In keeping with the work of other scholars on reducing surprise (Barnea, 2020; Handel, 1984), this shift further inspired my efforts to develop new models of sharing, anticipating, and imagining with the goal that strategic surprise need not be inevitable (Bray et al., 2009; Costigan, 2016c, 2016a; Costigan & Pallaris, 2016; Herd et al., 2013).

A. The New Domain of Cyberspace

Whereas crises may provide authorities with credible alerts and subsequent demands that signal a need for change, it is only since circa 2010 that the largely imperceptible, yet geometric, growth of cyberspace sparked concern from some quarters in defence and security studies. The nascent field of cyberspace studies created room for new paradigms, leading to the awareness that cyberspace is an entirely new defence domain (alongside land, air, sea, and space) with its own need for security (Brandes, 2013; Lynn III, 2010). For national and international security institutions, the act of conceiving of cyberspace as its own domain necessitated the development of new doctrines, definitions, educational objectives, and ultimately the training of personnel.

Since that initial point of definition, a combination of exogenous and endogenous factors, for example state-sponsored organised cybercrime (Bancroft, 2020; Gaidosch, 2018) and high-profile insider threats such as the cases of Edward Snowden and Chelsea Manning (Maasberg et al., 2020; Mazzarolo & Jurcut, 2019), have propelled cybersecurity to the forefront of national security and a prime global

security concern (Deibert, 2018; Reveron & Savage, 2020). While evidence suggests that the development of cyberspace may represent a fundamental shift in global affairs, more novel technologies continue to emerge as cyberspace maintains its radical rate of expansion (Costigan, 2016c, 2016a). The evolution of cyberspace is simultaneously altering societal capabilities as well as global dependence on new and legacy systems that are exposed to threats from state and non-state actors in areas as diverse as healthcare, finance, government, entertainment, defence, and critical infrastructures. To make matters more acute, my original research on technological and economic trends has indicated that the physical and virtual worlds appear to be merging (Costigan, 2016c; Costigan & Lindstrom, 2016), vastly expanding the available attack surface for cybercriminals and bad actors, while policymakers remain largely in the dark about such developments (Costigan, 2016c, 2016a).

In parallel with changes in security institutions' awareness, there is also increasing recognition among global elites and political authorities that cybersecurity issues should no longer be considered primarily technical in nature (Dunn Cavelty & Wenger, 2019). Concomitant with the changing views of political leadership, there is nascent awareness among cybersecurity experts that the initial bias of authorities towards technical solutions – to what was seen as a technical space – has proven widely insufficient to the demands placed on institutions that are charged with security (Costigan, 2016a; Costigan & Hennessy, 2016). Despite these realisations and apparent general agreement that cyberspace is a domain that requires normative, behavioural, legal, and doctrinal guidance for security and defence, security institutions remain deeply challenged over how to prioritise cybersecurity, as

well as how best to educate for change and thereby foster future leadership (Costigan, 2016c, 2016a; Costigan & Hennessy, 2016; Efthymiopoulos, 2019; Ilves et al., 2016).

B. Cyberspace and the History and Culture of Security Institutions

Cultural and historical legacies appear to play a significant role in how international security institutions come to understand their responsibilities. Contemporary security institutions were built in the wake of the World Wars, and their creation heralded what promised to become a new era of stability, economic prosperity, and peace. From neoliberal and critical perspectives, there is general agreement that these institutions were created largely with structures of control and predictable rules of engagement in mind (Lake, 2001). Yet cyberspace seemed to emerge *de novo,* challenging preconceived notions of stable developments. Further, even after the acceptance of cyberspace as a new domain, it remained branded as a 'Wild West', a portrayal that echoes in scholarship and policy work to this day. Working the analogy to its limits, defence academics and policymakers alike use the idea of the 'Wild West' to frame concepts like the expansion of cyberspace, apparent lawlessness, and the response of security institutions (a form of bringing the law) through the creation of cybersecurity (Chang et al., 2016; Costigan, 2021a; Finnie et al., 2010; Keyser, 2009).

As noted throughout my publications and related presentations, evidence indicates that institutional legacies and cultures, socio-technical factors, and conceptual biases inhibit authorities' acceptance of emerging security challenges, most notably for this commentary in the field of cybersecurity. These impediments often appear to be

significant deterrents to the resourcing and development of comprehensive, national and international responses to acute cybersecurity concerns, particularly to issues of current education for security practitioners and leadership (Bray et al., 2009; Costigan, 2016a; Herd et al., 2013).

IV. Frameworks for Conceptualisation and Operationalisation of Emerging Security Challenges

Conceived at a high level, the contours of security and defence educational institution learning agendas are historically set through guidance developed by policymakers and leadership (Guttieri, 2006; Lucena, 2005). In developing guidance for education, civilian leadership may work with academics and military officials at security and defence institutions who then typically hew curricular offerings to meet national educational objectives, a pattern that holds in modern democracies (Feaver & Kohn, 2000; Mukherjee, 2018). In addition to guidance, policymakers are also the primary source of funding and resources for defence educational endeavours. As such, policymakers hold a uniquely influential post that is also fraught with considerable risk, including the possibilities of wholesale omission of emerging challenges or suboptimal prioritisation relative to traditional, proximate, or most accepted concerns. For security and defence educational institutions to engage on new issues, policymakers must first recognize an emerging risk or opportunity and then transmit that guidance in the form of requests for further study, leading later to adaptive or revolutionary curricular changes and to the development of personnel fit to new circumstances.

A. Four-Factor Analytical Framework to Recognize and Situate Change

In recognition of the critical role of policymakers and the collective need to envision and act on mental models to anticipate and engage with change, I co-developed a four-factor analytical framework and an associated conceptual framework for policymakers to interrogate and frame emerging challenges (Herd et al., 2013). This framework allows policymakers to situate emerging challenges by noting their progression through temporal and other dimensions. I note that emerging security challenges often follow a pattern that policymakers may use to model the need for change in guidance or which may require further assessment:

1. **Creation of Authoritative Reports.** At this stage, scientific or technological reports are written that may then receive widespread attention but without yet moving to policy responses;
2. **Recognition of Change**. Some strategic threats – for example state-sponsored cybercrime or terrorism – may appear as rapidly mutating or enhanced by single or combinatorial technological developments, requiring the formation of new policy approaches and responses to address the new security challenges;
3. **Prioritization.** Longer-term challenges that might be dubbed ‘existential threats’, such as those from climate change or the use of nuclear weapons, may remain on the security agenda but may change position relative to more proximate, novel threats. New threats might still emerge as longer-term challenges but these can be considered to be emerging;
4. **Reprioritization.** Other identified emerging challenges may require policy responses but such responses might also come to be understood as

premature, leading to reprioritisation. Security for space-tourists would, for example, fall into this category while developing policy and education for cybersecurity in the space domain, or blockchain and cryptocurrency risks, might not.

It is important to underscore that the mental models of ‘change agents’ within the policy and defence communities are central to recognising the innovation/risk nexus and the potential need for change in guidance (Angerman, 2004; E. Rogers, 2010). As such, this framework was written in recognition of the role of policymakers to help improve outcomes through awareness and education.

B. Securitisation at the Point of Innovation: A Conceptual Framework

Technological life cycles continue to evolve and shorten. For the security and defence community, the effect of shortening development cycles is that emerging technological developments may rapidly mature before institutions are aware, guidance is written, or ‘securitisation’ has taken place (Herd et al., 2013; Webster & Gardner, 2019). These effects, combined with the risks of surprise as detailed above, suggest that policy and security institutions may need to think of securitisation alongside innovation. Compounding concerns, each successive wave of technological innovation comes with novel possibilities of recombination of existing technologies. Thereafter, exploitation – particularly by those with criminal intention or seeking advantages in security affairs – may occur while the next wave of technological change is almost directly behind. For example, consider the largely latent technologies and techniques of ransomware that – once combined with the invention of cryptocurrency – grew to become a challenge for nations and their

security institutions (Costigan & Gleason, 2019). Yet securitisation or regulation at the point of innovation may come with risks to industrial investment patterns and may, in some circumstances, also come to be considered a threat to progress (Aghion et al., 2021; Pelkmans & Renda, 2014; Rothwell, 1980). Recent scholarship in innovation systems literature suggests that recognition of 'transformational failures' may help improve innovation policy but scholarship on improving policy *interventions* is still nascent (Raven & Walrave, 2020).

As a part of my work as Senior Advisor to the NATO/Partnership for Peace Consortium (PfPC) Emerging Security Challenges Working Group, I co-developed a conceptual framework of trends and characteristics that shape awareness of the need for possible interventions in emerging and existing technologies. This conceptual framework employs descriptive categories and is intended for policymakers and others charged with staying abreast of innovations that may portend security impacts. The concepts and associated characteristics captured in this framework (Figure 1) are illustrative of the need for understanding and contextualising the potential impacts stemming from innovations. Additionally, trends and innovations may also be distinguished by multiple interrelationships and potential contradictions. As noted in this commentary, in their role as lead change agents, policymakers must keep pace with the potential or actual threats posed by innovations in order to know when to shape policies to mitigate risk or develop guidance for further analysis. To wit, while conducting a review of authoritative literature on innovation, policymakers may use this conceptual framework to ascertain the need for further observation, study, or the inclusion of new topics in educational programmes.

This framework is intended to be used alongside the review of authoritative reports to understand new risks, helping to identify when or how developments might become emerging security challenges. The characteristics listed in this framework may also assist policymakers and educators to more rapidly address issues of awareness and the likelihood of technological developments requiring new or renewed attention by security and defence educational institutions. Since its publication, this framework and the cross-disciplinary discourse that led it its development have been used in a variety of institutions and locales, with apparent applicability during the Covid-19 global pandemic, among other recent concerns (Ajdnik & Colten, 2013; Bester et al., 2020; Munro, 2020; Siriwardhane, 2019).

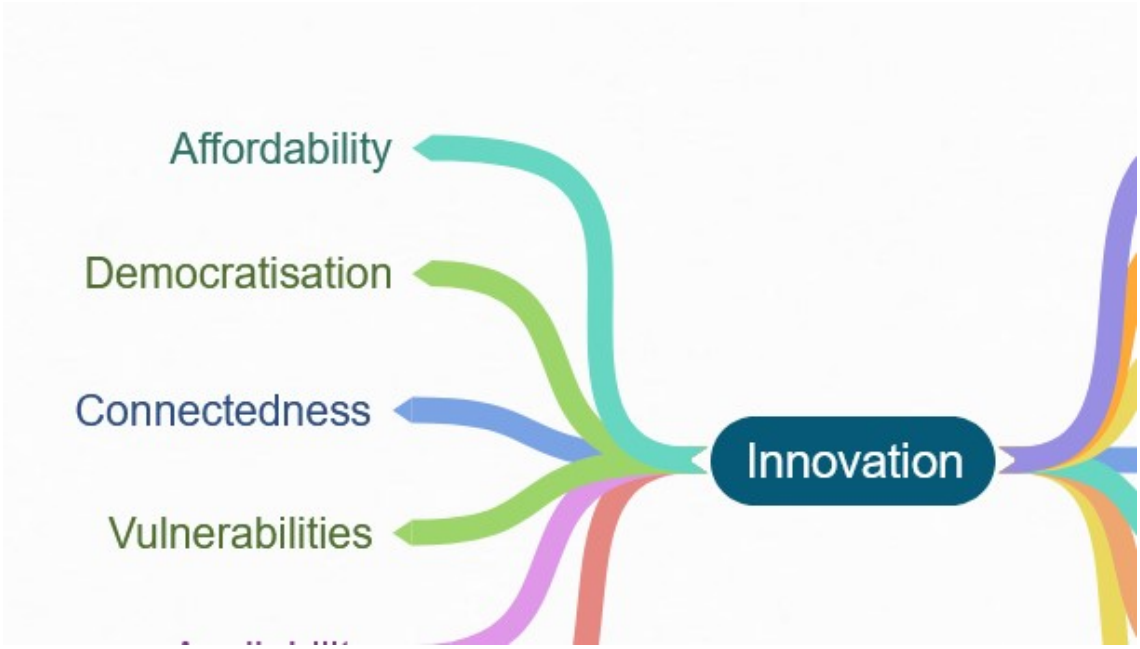

Figure 1: Innovation Framework for Policy Analysts

C. Situating Cybersecurity as a Hybrid Socio-Technical Domain

Since the genesis of cybersecurity as a new discipline and domain, considerable variability and subjectivity in terminology has been the norm (Branch, 2021; Craigen et al., 2014). While lexicographical differences often evince considerable challenges related to the creation of new domains of knowledge, some of these issues may be the result of generally increasing specialisation in academic fields of inquiry (M. Rogers, 2013). Specifically, the rapid innovations and dynamics surrounding cybersecurity allowed for the proliferation of terms, acronyms, and ultimately dividing lines, much of which was mirrored in military and state responses. This environment produced, in turn, a cloud of uncertainty with unbalanced or unevenly applied responses to cybersecurity challenges, potentially delivering and enshrining insecurity as a result (Alexander & Panguluri, 2017; Althonayan & Andronache, 2018). Presently, in many contemporary policy and academic discourse, there is growing realisation that while cybersecurity *emerged* from largely technical developments, with information technology and engineering disciplines dominating the early days, that pattern of 'issue ownership' may have significantly delayed political and legal scholarship into the security dimensions of cyberspace. As the initial imbalance became enshrined in scholarship, cybersecurity concerns continued to proliferate, growing to become one of the most complex socio-technical 'wicked problems' of the modern world (Carr & Lesniewska, 2020; Costigan, 2016a, 2016a; Costigan & Hennessy, 2016; Costigan & Lindstrom, 2016; Costigan & Perry, 2016; Stevens, 2018).

D. Framework for Socio-Technical Parity in Cybersecurity Education

To redress the imbalance between the technical and policy dimensions, I developed an original framework for cybersecurity education that – from the outset – creates greater parity in both the requisite technical pursuits and critical socio-political considerations needed to understand the security of cyberspace. This framework is central to *Cybersecurity: A Generic Reference Curriculum* published by NATO − hereafter referred to as the NATO Cybersecurity Reference Curriculum (Costigan & Hennessy, 2016). In developing this curriculum and framework, I drew inspiration from scholarship that underscores the value of framework-driven approaches to cybersecurity. The strengths of frameworks are well documented in the scholarly literature, indicating that frameworks help organisations both to properly orient their cybersecurity efforts as well as reinforce mutually beneficial realignment of social and technological practices (Alexander & Panguluri, 2017; Efthymiopoulos, 2019; Malatji et al., 2019).

In keeping with the vision to create a balanced framework, the NATO Cybersecurity Reference Curriculum addresses the fundamental challenges of educating for change in cybersecurity through four themes:

Theme 1: Cyberspace and the Fundamentals of Cybersecurity (which addresses structural components of cyberspace and their relationship to risk management).

Theme 2: Risk Vectors (which addresses vulnerabilities inherent to cyberspace and explorations of policy and management).

Theme 3: International Cybersecurity Organisations, Policies and Standards (which addresses international organisations and the ways in which these relate to national contexts and risk management).

Theme 4: Cybersecurity Management in the National Context (which addresses national cybersecurity management practices in depth).

The originality and utility of the NATO Cybersecurity Reference Curriculum (Costigan & Hennessy, 2016) framework approach to cybersecurity has been operationalised in many quarters, from community colleges to defence academies and national cybersecurity strategies around the world (Asgarov, 2021; A. Cabanlong, personal communication, 2022; Gawliczek, 2020; Kaloyanova, 2019; Rauchfuss, 2019; Ward, 2021).

V. Biases and Limiting Factors in International Security Institutions

For some institutions the ‘real’ emerging challenge may be defined as much by institutional and cultural change needed to enable more efficient, effective and legitimate educational and policy responses, as it is by the inherent complexity of the

challenges themselves (Bray et al., 2009; Costigan, 2016a; Costigan & Pallaris, 2016; Herd et al., 2013). Considerable scholarly attention has been paid to the hypothesis that military culture is inherently conservative, potentially leading security institutions to lack a culture of innovation. However, more recent scholarship questions those findings (Adamsky, 2010; Hill, 2015). My publications included in this commentary also expand and extend knowledge of security institutional deficiencies while offering potential remedies and proposed paths for new research.

In the field of cybersecurity many such impediments appear to be tied to biases, some of which are a result of legacies, cultures, or design and yet others are encoded in language of bureaucracies, scholarship, and policy choices. These barriers include:

- Widely apparent gender and age gaps in cybersecurity and defence education (Costigan, 2016a, 2021b; Costigan & Lark, 2020);
- Age-related prejudices that enshrine perceived virtues in youth or may casually consign personnel to certain types of work based on age (Costigan, 2016b, 2021b; Costigan & Lark, 2020);
- Inclinations to perceive cybersecurity as an exclusively technical field or even as a technical-first field versus a whole of government, techno-political-defence hybrid domain (Costigan, 2016b, 2016a, 2021b, 2021a; Costigan & Perry, 2016);
- Disparities in national cybersecurity objectives stemming from differing taxonomic and political visions of cyberspace (Costigan, 2016a, 2021c; Costigan & Hennessy, 2016);

- Differences in the interpretation of laws and application of norms (Costigan, 2016a);
- Cognitive biases that result in apparent limitations on the part of individual authorities to recognize change, even in the face of potentially existential security concerns. These issues also have impacts which are allied to the contributions detailed in this commentary (Acciarini et al., 2020; Bray et al., 2009; Costigan, 2016a).

Many of these findings extend from my publications; others emerge from my capacity building fieldwork. Additionally, several of these findings challenge common assumptions about international security institutions and their abilities to anticipate and manage change. During the development of the NATO Cybersecurity Reference Curriculum, the edited volume *Cyberspaces and Global Affairs*, my journal articles, research and field investigations, I sought to identify gaps in cybersecurity education that may weaken educational and policy responses. Several of these same gaps appear to militate against shared approaches to solutions that cut across traditional boundaries and cultures of governmental and military structures. In the development of the NATO Cybersecurity Reference Curriculum and subsequent field investigations, diverse institutional biases and cultures became evident, the most prevalent of which are detailed below.

The NATO Cybersecurity Reference Curriculum was created to fill a yawning gap in the educational support provided by NATO's Defence Education Enhancement Program (DEEP). NATO DEEP is 'a vehicle for reform' of allied and partner educational programs that, after the collapse of the Soviet Union and Warsaw Pact,

were mired in Soviet systems of pedagogy or were left to languish due to persistent, often dire, economic issues (Gawliczek, 2019; NATO, 2021). The creation of the NATO Cybersecurity Reference Curriculum made it possible for NATO DEEP to begin provisioning tailored, practical support to individual partner countries as they sought to develop cyber capacity and reshape their professional military education (PME) institutions to understand and manage present and future risk in this new domain. Now in broad use around the world, the knock-on effects of this curriculum have significantly contributed to knowledge of best practices in cybersecurity education, thereby directly improving the capacity of countries to provide for cybersecurity and directly facilitating advancements in international security through improved trust.

Historically, the development of the NATO Cybersecurity Reference Curriculum was far from assured. Despite the recognition of cyberspace as a new domain, as well as clear demand signals from partner nations, at NATO the development of a curriculum on cybersecurity lagged for a variety of institutional and political reasons. The production of reference curricula by NATO, and ultimately the placing of their imprimatur, cannot occur in a vacuum. After having overcome the first barrier – that of locating, transmitting and shepherding a request from the leadership of a partner nation (which in this case was Ukraine) that was judged to have sufficient need and meet with the consensus interests of Allied Nations – additional impediments held back its development.

The second barrier to the development of the NATO Cybersecurity Reference Curriculum was an amalgam of issues that were fundamental, socio-technical, and conceptual and which are detailed in this commentary. Fundamentally, NATO does

not ‘do *cybersecurity’* save for itself (Costigan & Hennessy, 2016). This stand is rooted in doctrinal and historical distinctions: NATO as an organisation was founded to provide collective self-defence, not ‘security’ per se where security and the priority of issues are conceived as national areas of competence. In short, NATO’s responsibility is to provide for collective *defence*. While the Emerging Security Challenges Division at NATO does recognize and do work on the issue of cybersecurity, there is little consensus on substantive issues, distinctions, or directions for the organisation (Burton, 2015; Chaudhary et al., 2018; Herd et al., 2013). In the face of a cyberattack that might significantly affect allies, NATO’s potential for response is both untested and largely undelineated, despite public statements such as that of NATO Secretary General Jens Stoltenberg: ‘A serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all’ (Stoltenberg, 2019). Most recently, when a series of attacks against Albania’s information infrastructures were attributed to Iran, NATO issued a public statement affirming support for Albania’s defence – to include countering via collective response – while also calling on all nations to uphold a norms-based approach to cyberspace.

Since NATO does not doctrinally encode the framing of cybersecurity as a collective issue, and in recognition that a curriculum on *cyberdefence* would not serve to meet broadly articulated needs of both partners and allies nor be in keeping with the standard lexicon across the emerging discipline, NATO would require substantial time to consider proposed ways forward. Thus, a seemingly small shift in language from *cyberdefence* (which is the only term of art encoded in NATO doctrine) to *cybersecurity* was sufficient to set off a series of political discussions that sought to answer the following: could a document that bears the imprimatur of NATO promote

the concept of cybersecurity? And would partners and allies mistake this shift in language and conflate support for cybersecurity educational development with expectations for collective cyberdefence? Would state and non-actors understand and accept the importance of these distinctions?

As I had primary responsibility for alerting NATO DEEP to a gap in institutional awareness relative to cybersecurity educational needs and then gathering requests from partner nations (which in the professional military education context are called 'demand signals') and in my capacity as Senior Advisor to the NATO/Partnership for Peace Consortium (PfPC) Working Group on Emerging Security Challenges, I was in a position to help navigate academic and political concerns in order to secure support from NATO's Emerging Security Challenges division. In this capacity, I was able to negotiate for acceptance of non-doctrinal, yet globally-accepted, standard frames of reference in lieu of further political positions. Once political agreement was reached on the necessity of a NATO curriculum on cybersecurity for partners, its development was to take place under the auspices of the Partnership for Peace Consortium of Defense Academies and Security Studies Institutes – a twenty-year old multilateral and governmentally-funded institution fostered by former U.S. Secretary of Defense William Cohen to be in 'the spirit of the Partnership for Peace'. This shift in the locus of development would prove instrumental, allowing both for greater flexibility than would likely be evident inside NATO while also satisfying further political requirements and partner needs.

From the outset of development, the curriculum was designed to facilitate high-level understanding of cybersecurity sufficient *for educators at organizations of any size* to

create standalone curricula for defence, military, and police academies. For the cybersecurity reference curriculum to be a success it had to achieve a level of abstraction. In effect, the curriculum needed to become a meta-curriculum that would bridge disciplinary divides while maintaining objective standards. From that standpoint, the curriculum would afford institutions the opportunity to tailor it to their cultural needs. The resulting book (Costigan & Hennessy, 2016) aimed to address cybersecurity broadly, but in sufficient depth, that non-technical experts would be able to develop a more complete picture of technological issues and technology experts could more completely appreciate national and international security and defence policy implications. The greatest challenge was creating an original curriculum that would fill cross-disciplinary gaps – being durable yet also forward-leaning – with the understanding that cybersecurity concerns may manifest with marked differences across NATO partner and ally space.

The development of the cybersecurity reference curriculum took place with the support of several partner nations (or those which are not yet part of the alliance). Notably, great interest was evidenced in the emerging field but there was also a pronounced lack of understanding of technologies that underpin cybersecurity, of policy gaps, and of threat and risk mitigation practises among national security and defence policy leaders. A similar gap in the understanding of national policy frameworks was identified among technical experts who sought to support the work or operationalise it in their institutions.

As noted in several of my publications, presentations on the development of the NATO Cybersecurity Reference Curriculum, and this commentary, my research

demonstrates that several biases, legacies, and cultures of knowing hamper broader gains in cybersecurity (Costigan, 2016b, 2016a, 2016c, 2021b; Costigan & Hennessy, 2016; Costigan & Lark, 2020; Costigan & Perry, 2016; Herd et al., 2013).

Principally, these are:

1. **Gender** — By any measure, the cybersecurity field remains largely a male enterprise. Global data collection on gender hiring is a considerable challenge which is compounded by definitional problems, e.g., what actually constitutes a 'cyber' job? Definitional challenges aside, government and military educational institutions – particularly defence academies – have the opportunity to narrow the gender gap. International and national security institutions are using various methods to improve these, many of which are detailed in a special issue of the U.S. Department of Defense journal *Per Concordiam* which I guest edited (Costigan & Lark, 2020). Since the publication of the NATO Cybersecurity Reference Curriculum and subsequent capacity-building efforts, defence education institutions in Botswana, Serbia, Moldova, Morocco, the Philippines, Tunisia, and Ukraine have expanded cybersecurity opportunities for all. The Serbian Defence Academy developed a particularly straightforward formula for successful recruitment: instead of simply relegating the problem to their future objectives – which could become a nebulous, untreated goal – they simply began by actively recruiting for gender diversity in their military and universities. By recruiting for diversity, they were able to achieve positive effects: in the Serbian defence academy, women now outnumber men in cybersecurity.

2. **Media Bias** — Legacies, biases, and journalistic practices appear to reflect the type of news stories most reported on issues of cybersecurity. Whether it is the trope of the hacker in a hoodie, poorly lit and alone in front of a computer, or news stories that conjure symbolic manifestations of catastrophic collapse (in keeping with the journalistic adage 'if it bleeds, it leads') the Fourth Estate has considerable power over what people see and digest. In addition to the static and overused imagery of a lone-wolf hacker, there appears to be a significant bias that manifests as more stories about Eastern European and Asian hackers than Western European or American cybercriminals. In the popular imagination and in the press, cyber threats and crimes remain largely a problem that emanates from abroad, very often from the former Soviet Bloc countries and, in particular, Russia. Stereotypes abound and unless grounded in fact, such reportage is apt to create blind spots in security education and policy responses (Costigan, 2016c, 2016a).

3. **Institutional Culture** — To a certain degree, receptivity to new challenges that stem from technological change appears to be tied to the structure and culture of institutions, which in turn affects the internal discourse of an institution and the diversity of knowledge brought to bear (Costigan & Pallaris, 2016). The interaction between internal socio-psychological, political, and cultural factors of international security institutions also appears to play a significant role in the development of education needed for understanding new risks and the training and hiring of personnel to meet security needs. With regard to the need for more trained cybersecurity professionals to fill the

global workforce gap (Costigan & Lark, 2020), what has emerged from my research is that government and military institutions have several advantages, notably the promise of job security, the potential for educational scholarships or loan repayment schemes, the prospect of lifelong training, and the values imbued by mission-driven organisational cultures (Costigan, 2021b).

4. **Age-related Biases** — The concepts of ‘digital native’ or ‘digital immigrant’ have been employed since the early days of the Internet, despite being problematic and without empirical support (Brown & Czerniewicz, 2010). Such rhetoric has become normalised in education, leading to false dichotomies that appear to stigmatise older generations, enshrine ageism as a virtue, reduce the available talent pool, and in general negatively affect hiring practices. While there have been strides in user interface development allowing for more rapid learning of new consumer technologies, it remains the case that no one is born knowing information technology nor with a rich understanding of risk. Furthermore, the digital native concept may be perceived as a bias against those coming from the developing world − or other ‘have nots’ − who may not have had ready access to information and communications technology (ICT), but may still be educated and available to treat cybersecurity issues. Equally, there are no policy savants. As my work conveys, it should follow that cybersecurity experts – where cybersecurity is conceived as a hybrid domain – need to be created through a combination of education in technology, policy, and other social sciences (Costigan, 2021b; Costigan & Hennessy, 2016; Costigan & Lark, 2020).

5. **Technical Training** — Often the talent for a security institution's cybersecurity efforts is drawn from military vocational training which tends to be highly technical and is often classified. Technical training, whether in military vocations or in defence academies, also often neglects socio-political and managerial concepts such as cultural and human factors, risk management, law, ethics, and policy. Given the well-documented global shortage of cybersecurity expertise, far too few public cybersecurity education programs exist. My work demonstrates that institutions of higher learning with graduate schools in public policy, social sciences, humanities, and sciences should endeavour to produce more interdisciplinary accredited programs in cybersecurity and other emerging security challenges. (Costigan, 2021b).

6. **Threat Actors and the Democratisation of Capabilities** — Analysts and experts alike appear to consistently underestimate the transformative potential of technology for threat actors. In my own research and publications, the trajectory of terrorist use of information and communications technologies follows an arc which could be analysed using the four-factor analytic framework for emerging security challenges: moving from the relatively straightforward use of ICT, to expertise in malicious hacking and the development of sophisticated influence operations. Definitional debates and traditionalist schools of thought continue to hamper security experts' understanding and resourcing of research into cyberterrorism, despite clear trend lines and authoritative reports. Most notably, my research underscores

the importance of understanding the democratisation of technologies and skills. As with other disruptive technologies that may impact socio-political and security concerns, the democratisation of technologies which once required skilled training have now moved to low cost, off the shelf, technologies with reduced barriers for entry (Costigan, 2016c, 2016a).

7. **Frameworks of Understanding** — Many different points of view, including cultural and socio-political, must be taken into account when discussing national and international cybersecurity. Widely divergent considerations inform national security organisations and their educational programmes. Emerging from my research, I note that many countries have developed their own terminology and eschewed widely used terminology as a matter of informed choice that may reflect national priorities versus international agreements or lexicons. An example of such a shift in national conceptualisations is the Russian view of 'information security'. In Russian doctrine, information security means controlling threats to people or institutions, versus the more common industrially accepted view of information security as the '*preservation of confidentiality, integrity, and availability of information'* (Costigan, 2021c; Costigan & Hennessy, 2016; *Information Security Based on ISO 27001/ISO 27002 - a Management Guide First Impression.*, 2009; International Organization for Standardization, 2022; Thomas, 2001). Failing to adopt standards worsens global cybersecurity risk and inhibits sharing against threats (Costigan, 2016a, 2021b; Costigan & Hennessy, 2016).

8. **International Differences** — For diplomats and others working in international cybersecurity, facility in cultural matters is crucial to gaining trust, particularly in countries and systems of government where cybersecurity is primarily a military or government security concern. Some governments are attempting to pursue national strategies that are underpinned by perceived ambiguity in cyberspace and international law. These agendas run contrary to the articulated interests of democracies and the global exchange of information. The major fear of some national governments appears to be that cyberspace might be used as a means to weaken rule, legitimacy, or trust in government (Costigan, 2021b; Costigan & Perry, 2016).

9. **Mainstreaming of Cybersecurity in Policy** — My publications detail that the prevailing assumption that cyberspace demands technical-first solutions is in contravention to the growing appreciation that ‘cyber’ is simply a prefix to what is otherwise predominantly collective political – albeit notional – space. As such, cyberspace has pronounced socio-political, security, and economic vulnerabilities, along with governmental and security institution responsibilities and perhaps, ultimately, remedies. While awareness of the need for conceptual change is growing in governments and militaries, this awareness is unequally distributed as risks increase exponentially (Costigan, 2016a, 2021a; Costigan & Lindstrom, 2016). These risks continue to offer openings for cybercriminals to expand their portfolios, while educational institutions continue to produce credentialed cybersecurity graduates who may not have

formal training in policy, social sciences, or laws. If cybersecurity is to become a normalised part of the policymaker's portfolio, then the socio-technical aspects of cybersecurity and policy should be integrated to a greater degree (Costigan, 2016a, 2021a).

10. **Legal Landscape** — There is wide variation in how nations address cybersecurity within domestic law. As with cultural elements, an overview of the structures and practices in international standards and requirements, as well as national cybersecurity concepts or legislation, is crucial to acceptance of tailored cybersecurity education. In short: one cannot airdrop a set of laws or regulations, it instead has to be developed (Costigan, 2021b). Further, there is but one international convention on cybercrime: the Budapest Convention on Cybercrime of the Council of Europe, with 66 signatories and another 15 countries set to become parties. The attribution challenge (a phrase that connotes the difficulties with tracking the source of threatening or illegal cyber activity) compounds problems as it requires technical capabilities that are unevenly distributed as well as legal authorities which might not be present. In this space, international security organisations may play a critical role in elevating the need for understanding and educating for legal and regulatory change in national contexts. For example, countries may come to be a signatory of the Budapest Convention or may come to understand the basics of attribution, often after being exposed to the opportunity during a capacity building effort sponsored by an international security institution or by talking with a trusted partner. Where international and regional security

organisations undertake educating partners, such positive knock-on effects are not uncommon.

Taken as a whole, as noted in my publications, these biases and limiting factors both point to the need for further research and assert that policymakers should seek the means and incentives to address them as matters of priority.

VI. Shifting the Query: from ‘So What?’ to ‘What if?’

As detailed above, in today’s unmediated, information-rich world, endogenous and exogenous challenges to the post-Cold War order have risen from many quarters, requiring security institutions to shift cultural attitudes, methods of education, and ways of knowing (Costigan, 2016a; Costigan & Pallaris, 2016; Costigan & Perry, 2016; G. Hall, 2020). Meanwhile, security institutions struggle to alter their cultures and the transformation of cybersecurity concerns continues unabated. For example, cybercrime, which is but one facet of cybersecurity, particularly startling changes are apparent when viewed retrospectively. My work focuses on these issues by considering, for example, the movement from lone-wolf hackers to centralised cartels and decentralised dark economies (Costigan, 2016a; Costigan & Gleason, 2019; Finnie et al., 2010; Gaidosch, 2018; Goodman, 2011; Holt, 2017; Wall, 2021). These changes have been enabled both by technological innovations and by criminal actors learning from each other in unmediated forums and sharing reports on how to exploit weaknesses in systems, institutional awareness, and economies (Bancroft, 2020; Taylor et al., 2019; Wall, 2021). Developed in my work, knowledge ecologies qua community networks of learning may be helping some international security institutions grasp change. Meanwhile, cybercriminals and terrorists have largely

embraced change, and in so doing, have become learning organizations with their own knowledge ecologies. Indeed, criminals have exhibited profound abilities to create and transfer knowledge across territorial, linguistic, and ideological boundaries (Costigan, 2016c; Costigan & Gleason, 2019; Costigan & Pallaris, 2016).

Starting in 2008 at The New School University's Graduate Program in International Affairs I developed and taught graduate level courses on international security and socio-political issues of cyberspace. At the time, such social science course offerings were extraordinarily rare in institutions of higher learning. However, such forward-leaning curricula were also keeping with The New School's dedication to progressive and critical intellectual, interdisciplinary inquiry (Friedlander, 2019; Rutkoff, 1988). As reflected on earlier in this commentary, wicked problems such as those evidenced by cybersecurity are interlocking and may be considered to be emerging when the wider academic and security community begin to debate them (Carr & Lesniewska, 2020; Herd et al., 2013; Rittel & Webber, 1974). Notably many academics were concerned primarily with cyberspace as something novel and therefore worthy of study and less with the securitisation of that space, risk, or impacts. Historical analysis shows that it was not until cybersecurity began being employed in national security policy documents that practitioners self-identified as 'cybersecurity experts' (Stevens, 2018).

Presently, courses of study in cyberspace or cybersecurity remain something of outliers at schools of public affairs, perhaps because cyberspace is dynamic, interdisciplinary and simultaneously contested space that is not easily relegated to one domain of knowledge or discipline (Deibert, 2018). The historical lineage matters

to this day, with impacts on how authorities and leadership have come to understand cybersecurity and who should study it. By many measures for those in the social sciences, ‘cyber’ was considered at best to be a tool and not a clear or legitimate area of inquiry, with possible exceptions for media and engineering departments which tend to support progressive, technology-first agendas. Today, engineering schools must also contend with social and cognitive layers to cybersecurity, with some experts articulating the need for a scientific understanding of the social aspects of cybersecurity and others noting the need to refocus on cybersecurity as social practice (Carley, 2020; Costigan, 2016a, 2021b; Dunn Cavelty, 2018). In short, for much of academia in the social sciences the focus is slowly shifting from what information and communication technology *does* to its impacts, which my original investigations and work have shown to be myriad (Costigan, 2016c, 2016a; Costigan & Lindstrom, 2016; Herd et al., 2013) and my original contributions in educational and curricular efforts have put into practice (Costigan, 2021b; Costigan & Hennessy, 2016; Costigan & Perry, 2016).

As with other emerging security challenges, awareness and interest in cyberspace and security concerns increased *after* impacts were felt by governmental and military institutions and became common topics for media reportage and authoritative reports. When confronted by new challenges which may be epistemic or disruptive, critics trained in the social sciences and traditionalist defence academics are apt to attempt to frame the challenge as one of a series of ‘so what?’ questions. Encoded in this form of query is the potential for dismissiveness or profound underestimation. Whereas my work sets out to ask a different variant based on foresight and risk: ‘What if?’ as in the formulations ‘What if technology X leads to social change Y?’ or

‘What if technology X isn’t a hyped development but instead is a genuine innovation that becomes wildly successful?’

In close cooperation with my publisher and working with one of my leading graduate students, I decided to develop a first of its kind primer on cybersecurity for students of policy and global affairs. The result was the book *Cyberspaces and Global Affair*s, first published in 2012, then acquired by Taylor & Francis and reprinted in 2016 (Costigan & Perry, 2016). Given the dynamism of cyberspace and the emerging cognizance of its impacts on international affairs, the attempt to capture the zeitgeist as an analogue-form primer presented several tests. Most notably, while scholarship was in its infancy on the political and security impacts of information and communications technologies, the selection and crafting of chapters had to reflect what was known at the time, as well as identify uncertainties about what the ongoing information revolution might portend. Distinct analytical and methodological approaches were required which, much like cyberspace, needed to be made amenable to sampling and reflection.

In the creation of the book, no field of study in *Cyberspace and Global Affairs* was more complex than security. One may draw an analogy to measurement in quantum physics here: in taking stock (or attempting to measure) real-time security concerns in cyberspace, shifting political realities were being affected by revolutions in ICT and by growing awareness – some of it perhaps hyped – of the ability of ICT to produce political change. For *Cyberspaces and Global Affairs* to be a successful primer, the publication was written to record positions as statements – of which some were intentionally provocative – as well as capture detailed scholarly examinations of political and security concerns. These positions, which in the book are called

viewpoints, offer forward-leaning or unconventional considerations as a way to tease out emerging cybersecurity issues with the intention to answer not only ‘so what?’ but ‘what if?’

As *Cyberspaces and Global Affairs* neared completion, world-changing events occurred throughout the Middle East, with ICT and social media taking centre stage. While the book and its timing might be considered prescient, the application of novel scholarly methods and shaping of hypotheses helped its success. Notably, as with other revolutions in socio-technical affairs, the political and security effects of both rapid innovation in information and communication technologies, and the adoption of such technologies, caught many governments largely unaware. Such surprises included the overthrow of governments, to include some of those of the Arab Spring, with reverberations felt through the Colour Revolutions to today. Critics are right to note that an overemphasis on technological drivers could serve to blindside institutional awareness of deprivations in basic physiological and economic needs, but I argue that fundamental changes enabled by the penetration and adoption of social media should not be easily dismissed or subsumed (Costigan & Perry, 2016).

For defence academies, pursuing ‘what if’ strategies of enquiry and understanding for wicked or interconnected problems that portend social-political change or possible crises is formidable. Even in more liberally-minded defence institutions, those who are charged with operational concerns may tend to dismiss academic enquiries as a form of ‘admiring the problem’. Bureaucratic and internal challenges mount while scholarly treatments require time, sufficient resourcing from authorities and, often, interdepartmental domain expertise. Securing resources and the requisite teams (and space) to accomplish multivariate analysis is a fundamental challenge,

as noted throughout this commentary. Yet, disruptive change continues to be the norm with impacts on security organisations, from terrorist and other criminal weaponisation of peace-time information and communication technologies, to pariah states and criminal gangs' adoption of innovative technologies.

For security practitioners, the potential geostrategic ramifications of cryptocurrencies and blockchain tracks what may be to the observer a now familiar pattern: from dismissals of a 'hype cycle' to realisation of actual change only after massive alteration has occurred. With cryptocurrencies and blockchain, the possibilities for circumventing controls and systems or creating new ways of illicit business (which are already affecting economics and politics) have become rich grounds for early adopters. Proponents of cryptocurrencies were clear about this radical proposition from the start of their experiment: advocates of cryptocurrencies and related technologies were in essence engineering a system to alter the entirety of money, global transactions, and economies. Yet what has gone widely ignored in the speculation around cryptocurrencies is the role that states play and their changing perspectives on the matter. In my journal article 'What If the Blockchain Cannot be Blocked?' my co-author and I analyse the geostrategic implications of a suite of technologies that has the possibility of altering core economic tenets about money and, along the way, further attracting the attention of those who would skirt the law. Change in and of itself is not new, and critics may counter that cryptocurrencies are in essence novelties relative to the scale of global investments and remittances (Costigan & Gleason, 2019, 2022; Hashemi Joo et al., 2019). However, as an example of how authorities underestimate the risks of technological developments, I posit that the blockchain and cryptocurrencies alter the way money functions and

that risks associated with these evolutions are potentially paradigm shifting (Costigan & Gleason, 2019, 2022).

With the blockchain, my analysis grapples with low probability/high impact possibilities which may indicate that the best time to pay attention is now. As with some other emerging challenges that are addressed in the cybersecurity education publications in this commentary, critics contend that the grand schemes of cryptocurrency and blockchain advocates have not come to fruition and may never be realised. This is a variant of the 'wait and see' strategy that traditionalists who work in support of national security may often maintain (Bray et al., 2009; Costigan, 2016a; Costigan & Pallaris, 2016; Herd et al., 2013). Cybercriminals and terrorists have already availed themselves of the strengths of cryptocurrency and, in so doing, now rival the illegal narcotic market in the scale of their proceeds and ambition (Costigan & Gleason, 2022; Liggett et al., 2020; Patel & Pereira, 2021; Roškot et al., 2021; Wang & Zhu, 2022). Similarly, since the publication of *Terrornomics* and my work on cyberterrorism, consistent and deliberate research has been done on new developments of cyberterrorism, placing it alongside other hybrid threats (Macdonald et al., 2019; Marsili, 2019; Plotnek & Slay, 2021). Awareness, generated either by events or scholarship on these issues, is likely to necessitate further changes in policy and cybersecurity education.

Traditionalists may argue that a new prioritisation of topics and resources may serve to detract from the orthodox curriculum that makes up the core of the current educational enterprise. It has also been suggested that changes to the curriculum may deliver unknown effects on future leadership, despite the criticality of educating

for uncertainty (Chow & Bowers, 2021; Comfort & Wukich, 2013; Slovic, 1986). In professional military education institutions, the pursuit of increased or topical cybersecurity offerings may remain framed as one of trade-offs. For example, in PME institutions some are quick to presuppose that cybersecurity educators would argue to 'displace studies of the Peloponnesian War in favour of emerging issues' even though, in my experience and in surveying the literature, no evidence of such radical shifts in educational programmes have come to light (Anonymous, personal communication, 2022; Marlatt, 2007; F. B. Schneider, 2013).

Cybersecurity education, as with those of other emerging security challenges, often remains rooted in longstanding cycles of repetitive behaviour (Herd et al., 2013; Mille, 2019) resulting in a walled garden that some in professional military education circles refer to as a 'geek ghetto'. In other settings this repetition of biases (for example, that cybersecurity is a technical field) may come to result in insecurity or even in 'security fatigue' (Reeves et al., 2021), leaving institutions in comparatively worse positions relative to shocks. My publications and research establish that cybersecurity educational programmes need to overcome substantial hurdles while remaining open to transdisciplinary approaches, foresight techniques and scholarship, and the effects of operating in uncertainty (Costigan, 2016a, 2021b; Costigan & Hennessy, 2016; Costigan & Pallaris, 2016).

VII. Conclusion

Emerging security challenges are unique in their capacity to surprise, often delivering markedly negative societal impacts. Whereas waiting for change may be the de facto position for many security institutions, without better anticipatory efforts policymakers

run risks of overreaction that may come after systemic shocks, costing society dearly. Having emerged from government-sponsored technical innovations to become one of society's most notable wicked problems, cyberspace and cybersecurity continues to evolve and challenge security institutions while national and global risks escalate. In the changing cybersecurity landscape, the need for balanced socio-technical knowledge, and the relative dearth of cybersecurity expertise, necessitates a fundamental shift in policy and educational priorities.

In my scholarship on cybersecurity, crime, and terrorism, as well as extensive field investigations and capacity building work that stem from publications considered in this commentary, what has emerged are novel hypotheses, conceptual frameworks, and impactful findings about present-day features in cybersecurity and related counter-crime education. My original contributions concentrate on institutional, socio-technical, and cultural factors in emerging challenges (Bray et al., 2009; Costigan, 2016a, 2016c; Herd et al., 2013), elucidating apparent impediments to improving outcomes while making original contributions to the growing body of scholarly literature on cybersecurity education, awareness, and resilience (Costigan & Gleason, 2019; Costigan & Hennessy, 2016; Costigan & Lindstrom, 2016; Costigan & Pallaris, 2016; Costigan & Perry, 2016).

Institutional cultures, doctrines, legacies and biases undoubtedly impact defence and security curriculum offerings (Costigan, 2016c, 2021b; Costigan & Pallaris, 2016). Traditionalist security academics, in their defence of more orthodox curricula, may come to underestimate the need for change. As a result, despite receiving purpose-built educations, those charged with security and defence may find themselves to be

poorly prepared to anticipate epistemic change. Policymakers, in their significant roles as gatekeepers for resources and guidance for new research and education, should also have the space, tools and frameworks to recognise and assess emerging challenges (Bray et al., 2009; Costigan, 2016c, 2016a; Costigan & Pallaris, 2016; Herd et al., 2013). As my publications detail, the education of a new class of anticipatory-minded, socio-technical security specialists appears paramount (Costigan, 2016a, 2016c, 2021b). Recognizing the significance of technological change may also be accomplished through a shift in mindset from potentially passing 'so what?' queries to the more open possibilities of impacts best addressed by the formulation 'what if?' In sum, my findings indicate that security institutions would benefit from employing knowledge ecologies and shared cognition to derive new value from lessons, question pathways, improve adaptation, and strengthen cultures of awareness.

To meet the need for long-term thinking and ration the worst effects of surprise, a more expansive view of education on emerging security challenges is required. Such an approach should also be ready to limit apprehensions that standard subject matters might be displaced in favour of restructuring for whatever new concern is on the horizon. While such innovations may not always be a matter for security education, technological shifts should be readily tested and studied. In parallel, guidance for new educational programmes should be pursued that allows for greater flexibility in adaptation to change. As noted in my publications, failing to alter educational and awareness patterns appears to buttress institutional and cognitive barriers that keep cybersecurity and other socio-technical challenges in a walled

garden while societal costs increase (Costigan, 2016c, 2016a, 2021b; Costigan & Perry, 2016).

Guidance, such as the conceptual framework on innovation and securitisation cited herein, has the prospect of further assisting policymakers in their recognition and prioritisation of emerging risks that stem from technological developments. Likewise, the framework I developed for NATO's Cybersecurity Reference Curriculum serves as a model and guide for national governments to alleviate some of the more pervasive risks and imbalances. There are significant challenges that manifest differently across different institutional cultures, but some of these challenges can be remedied by sustained effort to reduce barriers while simultaneously recognizing biases that shape our thinking.

Change is inevitable and surprise may be part of the human condition. However, further transdisciplinary scholarship may yet reveal pathways to improve anticipation and resilience to strategic surprise. Nonetheless, as my doctoral-level publications and research demonstrate, the effectiveness of a multi-pronged approach to address present-day shortcomings in cybersecurity education is not simply a matter of avoiding surprise but is rather a goal to systematically redress imbalances in cybersecurity as a whole. As my work also details, addressing cybersecurity as a harmonised socio-technical domain does not obviate nor argue against the need for deep technical or social science expertise. It does, however, indicate that cybersecurity concerns remain wicked problems that may yet be amenable to being addressed by new frameworks, guidance, and transdisciplinary educational approaches (Costigan, 2016a; Costigan & Hennessy, 2016; Herd et al., 2013).

The Spanish-American philosopher George Santyana once noted that to ‘see better what we now see, to see by anticipation what we should see actually under other conditions, is wonderfully [sic] to satisfy curiosity and to enlighten conduct’ (Santayana, 1906). In that spirit, I have shown that defence and security academics working in international security institutions and in cooperation with policymakers have the opportunity to improve anticipation, generate awareness, and facilitate the conditions for better educational and societal outcomes. It is my hope that my scholarly contributions to the field of security will continue to help others to imagine, educate, and plan for better futures.

References

Acciarini, C., Brunetta, F., & Boccardelli, P. (2020). Cognitive biases and decision-making strategies in times of change: A systematic literature review. *Management Decision*. https://doi.org/10.1108/md-07-2019-1006

Adamsky, D. (2010). *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel.* Stanford University Press. https://doi.org/10.1515/9780804773805

Aghion, P., Bergeaud, A., & Van Reenen, J. (2021). *The Impact of Regulation on Innovation* (No. w28381; p. w28381). National Bureau of Economic Research. https://doi.org/10.3386/w28381

Ajdnik, L., & Colten, K. (2013, September). Review: Emerging Security Challenges: Framing the Policy Context. *Federation of American Scientists*. https://fas.org/blogs/fas/2013/09/review-emerging-security-challenges-framing-policy-context

Alemanno, A. (2018). How to Counter Fake News? A Taxonomy of Anti-fake News Approaches. *European Journal of Risk Regulation*, *9*(1), 1–5. https://doi.org/10.1017/err.2018.12

Alexander, R. D., & Panguluri, S. (2017). Cybersecurity Terminology and Frameworks. In R. M. Clark & S. Hakim (Eds.), *Cyber-Physical Security* (pp. 19–47). Springer International Publishing. https://doi.org/10.1007/978-3-319-32824-9_2

Alizadeh, M., Shapiro, J. N., Buntain, C., & Tucker, J. A. (2020). Content-based features predict social media influence operations. *Science Advances*, *6*(30), eabb5824. https://doi.org/10.1126/sciadv.abb5824

Althonayan, A., & Andronache, A. (2018). Shifting from Information Security towards a Cybersecurity Paradigm. *Proceedings of the 2018 10th International Conference on Information Management and Engineering - ICIME 2018*, 68–79. https://doi.org/10.1145/3285957.3285971

Angerman, W. (2004). *Coming full circle with Boyd's OODA loop ideas: An analysis of innovation diffusion and evolution*. Air University.

Anonymous. (2022). *Cybersecurity Education in US PME Institutions* [Personal communication].

Anthony, M. C. (Ed.). (2016). *An introduction to non-traditional security studies: A transnational approach*. Sage.

Asgarov, R. (2021). *NATO'nun Siber Uzay Operasyonları: Tehditlere Karşı Yeni Stratejiler* (No. 35). https://www.ulusam.org.tr/wp-content/uploads/2021/04/NATO-Siber-Guvenlik-Politikasi.pdf

Bancroft, A. (2020). Cybercrime is not always rational, but it is reasonable. In *The Darknet and Smarter Crime*. Palgrave.

Barnard-Wills, D., & Ashenden, D. (2012). Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture*, *15*(2), 110–123. https://doi.org/10.1177/1206331211430016

Barnea, A. (2020). Strategic intelligence: A concentrated and diffused intelligence model. *Intelligence and National Security*, *35*(5), 701–716. https://doi.org/10.1080/02684527.2020.1747004

Bester, P. C., Els, S., & Olivier, L. (2020). Deployment of the South African National Defence Force for COVID-19: A Case Study on Governance. *Africa Journal of Public Sector Development and Governance*, *3*(1), 105.

Birkland, T. A. (1997). *After disaster: Agenda setting, public policy, and focusing events*. Georgetown University Press.

Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2019). Educating Future Multidisciplinary Cybersecurity Teams. *Computer*, *52*(3), 58–66. https://doi.org/10.1109/MC.2018.2884190

Bonk, C., & Graham, C. (2012). *The Handbook of Blended Learning: Global Perspectives, Local Designs*. John Wiley & Sons.

Boyne, G. A., & Entwistle, T. (Eds.). (2010). *Public service improvement: Theories and evidence*. Oxford University Press.

Branch, J. (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization*, *75*(1), 39–70. https://doi.org/10.1017/S002081832000051X

Brandes, S. (2013). The newest warfighting domain: Cyberspace. *Synesis: Science, Technology, Ethics, Policy*, *4*. https://doi.org/10.1.1.1049.5627&rep=rep1&type=pdf

Bray, D. A., Costigan, S., Daum, K. A., Lavoix, H., Malone, E. L., & Pallaris, C. (2009). Perspective: Cultivating Strategic Foresight for Energy and Environmental Security. *Environmental Practice*, *11*(3), 209–211. https://doi.org/10.1017/s1466046609990081

Brown, C., & Czerniewicz, L. (2010). Debunking the 'digital native': Beyond digital apartheid, towards digital democracy. *Journal of Computer Assisted Learning*, *26*(5), 357–369. https://doi.org/10.1111/j.1365-2729.2010.00369.x

Burton, J. (2015). NATO's cyber defence: Strategic challenges and institutional adaptation. *Defence Studies*, *15*(4), 297–319. https://doi.org/10.1080/14702436.2015.1108108

Cabanlong, A. (2022). *Government of Philippines: NATO Cybersecurity Reference* [Personal communication].

Callan, B., Costigan, S., & Keller, K. (1997). *Exporting U.S. High Tech, Facts & Fiction About the Globalization of Industrial R&D*. Council on Foreign Relations Press ; Distributed by Brookings Institution Press.

Carley, K. M. (2020). Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9

Carr, M., & Lesniewska, F. (2020). Internet of Things, cybersecurity and governing wicked problems: Learning from climate change governance. *International Relations*, *34*(3), 391–412. https://doi.org/10.1177/0047117820948247

Ceruzzi, P. E. (2003). *A history of modern computing* (2nd ed.). The MIT Press.

Chang, L. Y. C., Zhong, L. Y., & Grabosky, P. N. (2016). Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance*, *12*(1), 101–114. https://doi.org/10.1111/rego.12125

Chaudhary, T., Jordan, J., Salomone, M., & Baxter, P. (2018). Patchwork of confusion: The cybersecurity coordination problem. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy005

Chow, A., & Bowers, J. (2021). Educating for what? PME, the ADF and an uncertain 21st century. *The Centre of Gravity Series*.

Christensen, C., Raynor, M., & McDonald, M. (2013). Disruptive innovation. *Harvard Business Review*.

Christianson, M. K., & Barton, M. A. (2021). Sensemaking in the Time of COVID□19. *Journal of Management Studies*, *58*(2), 572–576. https://doi.org/10.1111/joms.12658

Cohen, E. A., & Gooch, J. (2006). *Military misfortunes: The anatomy of failure in war* (1st Free Press pbk. ed). Free Press.

Comfort, L. K., & Wukich, C. (2013). Developing Decision-Making Skills for Uncertain Conditions: The Challenge of Educating Effective Emergency Managers. *Journal of Public Affairs Education*, *19*(1), 53–71. https://doi.org/10.1080/15236803.2013.12001720

Cordey, S. (2019). *Cyber Influence Operations: An Overview and Comparative Analysis* (p. 38 p.) [Application/pdf]. ETH Zurich. https://doi.org/10.3929/ETHZ-B-000382358

Costigan, S. (2016a). Cybersecurity, Global Governance and New Risk. In *India's Approach to Asia* (pp. 343–363). Pentagon Press. https://idsa.in/book/indias-approach-to-asia-strategy-geopolitics-and-responsibility

Costigan, S. (2016b). *Eight Lessons from a Cybersecurity Curriculum*. https://www.linkedin.com/pulse/eight-lessons-from-cybersecurity-curriculum-sean-costigan

Costigan, S. (2016c). Terrorists and the Internet: Crashing or cashing in? In *Terrornomics* (pp. 113–129). Routledge. 2016. (Original Work Published 2007)

Costigan, S. (2021a). Charting a New Path for Cybersecurity After SolarWinds. *The Diplomatic Courier*. https://www.diplomaticourier.com/posts/charting-a-new-path-for-cybersecurity-after-solarwinds

Costigan, S. (2021b). *Cyber Education and Institutions*. Cyber Education and Institutions 2021

Costigan, S. (2021c). Sovereign or Global Internet? Russia and China Press for Cybercrime Treaty. *Connections: The Quarterly Journal*, *20*(2), 9–13.

Costigan, S., & Gleason, G. (2019). What If Blockchain Cannot Be Blocked? Cryptocurrency and International Security. *Information & Security: An International Journal*, *43*(1). https://isij.eu/article/what-if-blockchain-cannot-be-blocked-cryptocurrency-and-international-security

Costigan, S., & Gleason, G. (2022, March 24). The Rise of Crypto and How it Disrupts Currency Systems. *The Diplomatic Courier*. https://www.diplomaticourier.com/posts/examining-the-rise-of-crypto-and-how-it-disrupts-currency-systems

Costigan, S., & Hennessy, M. A. (2016). *Cybersecurity: A Generic Reference Curriculum*. NATO.

Costigan, S., & Lark, P. (2020). Cybersecurity Workforce Development. *Per Concordiam*, *10*(4). https://perconcordiam.com/v10n4-eng/

Costigan, S., & Lindstrom, G. (2016). Policy and the Internet of Things. *Connections: The Quarterly Journal*, *15*(2), 9–18. https://doi.org/10.11610/connections.15.2.01

Costigan, S., & Pallaris, C. (2016). Knowledge Ecologies in International Affairs: A New Paradigm for Dialog and Collaboration. In *Cyberspaces and Global Affairs* (pp. 283–293). Routledge. https://ui.adsabs.harvard.edu/abs/2012arXiv1201.1928C/abstract (Original Work Published 2012)

Costigan, S., & Perry, J. (2016). *Cyberspaces and Global Affairs* (1st ed.). Routledge. (Original Work Published 2012)

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Daneshmandnia, A. (2019). The influence of organizational culture on information governance effectiveness. *Records Management Journal*, *29*(1/2), 18–41. https://doi.org/10.1108/RMJ-09-2018-0033

Dawes, S. S., Cresswell, A. M., & Pardo, T. A. (2009). From “Need to Know” to “Need to Share”: Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks. *Public Administration Review*, *69*(3), 392–402. https://doi.org/10.1111/j.1540-6210.2009.01987_2.x

Deibert, R. (2018). Trajectories for future cybersecurity research. In *The Oxford Handbook of International Security*. Oxford.

Dombrowski, P., & Gholz, E. (2006). *Buying Military Transformation Technological Innovation and the Defense Industry*. Columbia University Press.

Dombrowski, P., & Gholz, E. (2009). *Identifying disruptive innovation: Innovation theory and the defense industry* (Innovations: Technology, Governance, Globalization). SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1431506

Dreyer, I., & Stang, G. (2013). Foresight in governments–practices and trends around the world. In *Yearbook of European Security*.

Dumaine, C., & Mintzer, I. (2015). Confronting Climate Change and Reframing Security. *The SAIS Review of International Affairs*, *35*(1), 5–16.

Dunn Cavelty, M. (2018). Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance*, *6*(2), 22–30. https://doi.org/10.17645/pag.v6i2.1385

Dunn Cavelty, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855

Dyson, T. (2019). The military as a learning organisation: Establishing the fundamentals of best-practice in lessons-learned. *Defence Studies*, *19*(2), 107–129. https://doi.org/10.1080/14702436.2019.1573637

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, *8*(1). https://doi.org/10.1186/s13731-019-0105-z

Farrell, T., & Terriff, T. (Eds.). (2002). *The sources of military change: Culture, politics, technology*. Lynne Rienner Publishers.

Feaver, P. D., & Kohn, R. H. (2000). The Gap: Soldiers, Civilians and their Mutual Misunderstanding. *The National Interest*, *61*, 29–37. JSTOR.

Finnie, T., Petee, T., & Jarvis, J. (2010). *Future Challenges of Cybercrime*. Proceedings of the Futures Working Group.

Friedlander, J. (2019). *A Light in Dark Times: The New School for Social Research and Its University in Exile*. Columbia University Press.

Gaidosch, T. (2018, June). The Industrialization of CYBERCRIME: Lone-wolf hackers yield to mature businesses. *Finance & Development*, *55*(2), 22+. Gale Academic OneFile.

Gawliczek, P. (2019). Innovative ICT solutions and/within/for changing security environment. Case study – NATO DEEP ADL Portal and Social Media. *Journal of Scientific Papers 'Social Development and Security'*, *9*(4). https://doi.org/10.33445/sds.2019.9.4.8

Gawliczek, P. (2020). E-Learning as a Tool to Support Cybersecurity Education. *Civitas Et Lex*, *25*(1).

Goodman, M. (2011). International Dimensions of Cybercrime. In S. Ghosh & E. Turrini (Eds.), *Cybercrimes: A Multidisciplinary Analysis* (pp. 311–339). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-13547-7_17

Gouré, D. (2018). *Winning Future Wars: Modernization and a 21st Century Defense Industrial Base*. The Heritage Foundation. https://www.heritage.org/military-strength-topical-essays/2019-essays/winning-future-wars-modernization-and-21st-century

Grabher, G. (2004). Temporary Architectures of Learning: Knowledge Governance in Project Ecologies. *Organization Studies*, *25*(9), 1491–1514. https://doi.org/10.1177/0170840604047996

Grusin, R. A. (2010). *Premediation: Affect and mediality after 9/11*. Palgrave Macmillan.

Guttieri, K. (2006). Chapter 9 Professional Military Education in Democracies. In T. C. Bruneau & S. D. Tollefson (Eds.), *Who Guards the Guardians and How* (pp. 235–262). University of Texas Press. https://doi.org/10.7560/712782-012

Hall, A. (2017). Investing in Cybersecurity Solutions. *The Cyber Defense Review*, *2*(2), 9–12.

Hall, G. (2020). *NATO's post-Cold war transformation: Exploring change in counter-insurgency, collective defence, and cyber-security*.

Handel, M. I. (1984). Intelligence and the problem of strategic surprise*. *Journal of Strategic Studies*, *7*(3), 229–281. https://doi.org/10.1080/01402398408437190

Hashemi Joo, M., Nishikawa, Y., & Dandapani, K. (2019). Cryptocurrency, a successful application of blockchain technology. *Managerial Finance*, *46*(6), 715–733. https://doi.org/10.1108/MF-09-2018-0451

Head, B. (2022). Coping with wicked problems in policy design. In B. Peters & G. Fontaine (Eds.), *Research Handbook of Policy Design*. Edward Elgar Publishing. https://doi.org/10.4337/9781839106606

Herd, G., Puhl, D., & Costigan, S. (2013). *Emerging Security Challenges: Framing the Policy Context*.

https://dam.gcsp.ch/files/2y109l9BLlhXU8qQPsVDeTeBuJZGJm7MMN0vB9FmQm3EPmvW5dfdR2

Hill, A. (2015). Military Innovation and Military Culture. *The US Army War College Quarterly: Parameters*, *45*(1).

Holt, T. J. (2017). *Cybercrime through an interdisciplinary lens*. Routledge, Taylor & Francis Group.

Hurel, L. M., & Lobato, L. C. (2021). Keeping silos or building bridges? *COMPANION TO GLOBAL CYBER-SECURITY STRATEGY*, 504.

Hussain, A., Mohamed, A., & Razali, S. (2020). A Review on Cybersecurity: Challenges & Emerging Threats. *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, 1–7. https://doi.org/10.1145/3386723.3387847

Ilves, L., Evans, T. J., Cilluffo, F. J., & Nadeau, A. A. (2016). European Union and NATO Global Cybersecurity Challenges: A Way Forward. *PRISM*, *6*(2), 126–141.
Information Security Based on Iso 27001/Iso 27002—A Management Guide First Impression. (2009). Van Haren Pub.

International Organization for Standardization. (2022, May 12). *ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements*. ISO.
https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/45/54534.html

Kaiser, R. (2015). The birth of cyberwar. *Political Geography*, *46*, 11–20.
https://doi.org/10.1016/j.polgeo.2014.10.001

Kaloyanova, K. (2019). Exploring Cybersecurity Curricula Designation Requirements. *Computer and Communications Engineering*, *13*(2), 64–68.

Kean, T. H., Hamilton, L., & On, C. (2004). *The 9/11 Commission report: Final report of the National Commission on Terrorist Attacks upon the United States*. National Commission On Terrorist Attacks Upon The United States.

Keyser, Mi. (2009). Future Challenges of Cybercrime. In *Computer Crime* (pp. 287–326). Routledge.

Kuhn, T. S. (1962). *The Structure of Scientific Revolutions*. University of Chicago Press.
https://doi.org/10.7208/chicago/9780226458144.001.0001

Lake, D. A. (2001). Beyond Anarchy: The Importance of Security Institutions. *International Security*, *26*(1), 129–160. https://doi.org/10.1162/016228801753212877

Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2020). The Dark Web as a Platform for Crime: An Exploration of Illicit Drug, Firearm, CSAM, and Cybercrime Markets. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and*

Cyberdeviance (pp. 91–116). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_17

Lindsay, J. R. (2020). *Information Technology and Military Power*. Cornell University Press. https://doi.org/10.1515/9781501749582

Lucena, J. C. (2005). *Defending the nation: US policymaking to create scientists and engineers from Sputnik to the 'War against Terrorism'*. University Press America.

Lynn III, W. F. (2010). Defending a new domain—The Pentagon's cyberstrategy. *Foreign Affairs*, *89*, 97.

Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. *Communications of the ACM*, *63*(12), 64–80. https://doi.org/10.1145/3408864

Macdonald, S., Jarvis, L., & Lavis, S. M. (2019). Cyberterrorism Today? Findings From a Follow-on Survey of Researchers. *Studies in Conflict & Terrorism*, 1–26. https://doi.org/10.1080/1057610X.2019.1696444

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*, *27*(2), 233–272. https://doi.org/10.1108/ICS-03-2018-0031

Malhotra, Y. (2002). *Information ecology and knowledge management: Toward knowledge ecology for hyperturbulent organizational environments*. Syracuse University.

Mandrick, B., & Smith, B. (2022). Philosophical foundations of intelligence collection and analysis: A defense of ontological realism. *Intelligence and National Security*, 1–11. https://doi.org/10.1080/02684527.2022.2076330

Maor, M. (2017). Rhetoric and doctrines of policy over- and underreactions in times of crisis. *Policy & Politics*. https://doi.org/10.1332/030557317X14843233064353

Marlatt, G. (2007). *A Bibliography of Professional Military Education (PME)*. Dudley Knox Library. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.371.4682&rep=rep1&type=pdf

Marsh, D., & McConnell, A. (2010). Towards a framework for establishing policy success. *Public Administration*, *88*(2), 564–583.

Marsili, M. (2019). The War on Cyberterrorism. *Democracy and Security*, *15*(2), 172–199. https://doi.org/10.1080/17419166.2018.1496826

Massumi, Brian. (2007). Potential Politics and the Primacy of Preemption. *Theory & Event*, *10*(2). https://doi.org/10.1353/tae.2007.0066

Mazzarolo, G., & Jurcut, A. D. (2019). *Insider threats in Cyber Security: The enemy within the gates*. https://doi.org/10.48550/ARXIV.1911.09575

Mendelsohn, E., Smith, M. R., & Weingart, P. (1988). *Science, Technology and the Military*. Springer Netherlands. https://doi.org/10.1007/978-94-017-2958-1

Mille, E. M. (2019). *Perceptions of Military Personnel Regarding Workplace Disruptions in the Fourth Industrial Revolution*. University of Johannesburg.

Mitroff, I. I. (1988). Crisis management: Cutting through the confusion. *MIT Sloan Management Review*, *29*(2).

Mitroff, I. I., Shrivastava, P., & Udwadia, F. E. (1987). Effective crisis management. *Academy of Management Perspectives*, *1*(4), 283–292.

Mukherjee, A. (2018). Educating the Professional Military: Civil–Military Relations and Professional Military Education in India. *Armed Forces & Society*, *44*(3), 476–497. https://doi.org/10.1177/0095327X17725863

Munro, E. (2020). *Strengthening Prevention with Better Anticipation: COVID-19 and Beyond* (No. 9). Geneva Centre for Security Policy. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/GCSP_Strengthening-Prevention-with-Better-Anticipation.pdf

NATO. (2021, April 19). *NATO Defence Education Enhancement Programme develops a strategy in support of professional military education*. NATO. https://www.nato.int/cps/en/natohq/news_183394.htm

Patel, P. C., & Pereira, I. (2021). The relationship between terrorist attacks and cryptocurrency returns. *Applied Economics*, *53*(8), 940–961. https://doi.org/10.1080/00036846.2020.1819952

Pelkmans, J., & Renda, A. (2014). *Does EU regulation hinder or stimulate innovation?* Centre for European Policy Studies. https://EconPapers.repec.org/RePEc:eps:cepswp:9822

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning*, *12*(3), 224–232.

Plotnek, J. J., & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. *Computers & Security*, *102*, 102145. https://doi.org/10.1016/j.cose.2020.102145

Rauchfuss, G. (2019, February). *Designing the Curriculum*. AMEP Faculty and Curriculum Development Workshop, Accra, Ghana. https://africacenter.org/programs/amep-faculty-and-curriculum-development-workshop/

Raven, R., & Walrave, B. (2020). Overcoming transformational failures through policy mixes in the dynamics of technological innovation systems. *Technological Forecasting and Social Change*, *153*, 119297. https://doi.org/10.1016/j.techfore.2018.05.008

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue. *SAGE Open*, *11*(1), 215824402110000. https://doi.org/10.1177/21582440211000049

Reveron, D. S., & Savage, J. E. (2020). Cybersecurity Convergence: Digital Human and National Security. *Orbis*, *64*(4), 555–570. https://doi.org/10.1016/j.orbis.2020.08.005

Rittel, H. W., & Webber, M. M. (1974). Wicked Problems. *Man-Made Futures*. https://cms1files.revize.com/mncounties/document_center/Committees/Wicked%20Problems%20Summary%20Handout.pdf

Rogers, E. (2010). *Diffusion of Innovations* (4th ed.). Simon and Schuster.

Rogers, M. (2013). What is a 'domain' and is this a useful question? *ASp*, *64*, 5–16. https://doi.org/10.4000/asp.3810

Roškot, M., Wanasika, I., & Kreckova Kroupova, Z. (2021). Cybercrime in Europe: Surprising results of an expensive lapse. *Journal of Business Strategy*, *42*(2), 91–98. https://doi.org/10.1108/JBS-12-2019-0235

Rothwell, R. (1980). The impact of regulation on innovation: Some U.S. data. *Technological Forecasting and Social Change*, *17*(1), 7–34. https://doi.org/10.1016/0040-1625(80)90055-4

Rumsfeld, D. H. (2002). Transforming the Military. *Foreign Affairs*, *81*(3), 20. https://doi.org/10.2307/20033160

Rutkoff, P. (1988). *New School: A History of the New School of Social Research*. Free Press.

Santayana, G. (1906). *Reason in science*. Dover.

Schneider, F. B. (2013). Cybersecurity Education in Universities. *IEEE Security & Privacy*, *11*(4), 3–4. https://doi.org/10.1109/MSP.2013.84

Schneider, J. (2019). The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war. *Journal of Strategic Studies*, *42*(6), 841–863. https://doi.org/10.1080/01402390.2019.1627209

Sen, R. (2018). Challenges to Cybersecurity: Current State of Affairs. *Communications of the Association for Information Systems*, 22–44. https://doi.org/10.17705/1CAIS.04302

Si, S., & Chen, H. (2020). A literature review of disruptive innovation: What it is, how it works and where it goes. *Journal of Engineering and Technology Management*, *56*, 101568. https://doi.org/10.1016/j.jengtecman.2020.101568

Siriwardhane, I. (2019). *Key International Security Challenges in Contemporary Global Politics*.

Slovic, P. (1986). Informing and Educating the Public About Risk. *Risk Analysis*, *6*(4), 403–415. https://doi.org/10.1111/j.1539-6924.1986.tb00953.x

Solar, C. (2020). Cybersecurity and cyber defence in the emerging democracies. *Journal of Cyber Policy*, *5*(3), 392–412. https://doi.org/10.1080/23738871.2020.1820546

Stevens, T. (2018). Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance*, *6*(2), 1–4. https://doi.org/10.17645/pag.v6i2.1569

Stoltenberg, J. (2019). NATO Will Defend Itself. *Prospect*, 4.

Stuart, M. T. (2022). Scientists are Epistemic Consequentialists about Imagination. *Philosophy of Science*, 1–22. https://doi.org/10.1017/psa.2022.31

Sylves, R. (2005). Why revolutionary change is needed in emergency management. *Journal of Emergency Management*, *3*(6).

Taleb, N. N. (2007). *The black swan: The impact of the highly improbable* (1st ed). Random House.

Taleb, N. N. (2014). *Antifragile: Things that gain from disorder*. Random House Trade Paperbacks.

Taylor, R. W., Fritsch, E. J., Liederbach, J., Saylor, M. R., & Tafoya, W. L. (2019). *Cyber crime and cyber terrorism*. Pearson.

Thomas, T. L. (2001). Information security thinking: A comparison of US, Russian, and Chinese concepts. *Foreign Military Studies Office*.

Vacca, W. A. (2011). Military Culture and Cyber Security. *Survival*, *53*(6), 159–176. https://doi.org/10.1080/00396338.2011.636520

Vishik, C., & Balduccini, M. (2015). Making Sense of Future Cybersecurity Technologies: Using Ontologies for Multidisciplinary Domain Analysis. In H. Reimer, N. Pohlmann, & W. Schneider (Eds.), *ISSE 2015* (pp. 135–145). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-10934-9_12

Wall, D. S. (2021). *The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in Ransomware Offender Tactics, Attack Scalability and the Organisation of Offending*. papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3908159

Walt, S. M. (1991). The Renaissance of Security Studies. *International Studies Quarterly*, *35*(2), 211. https://doi.org/10.2307/2600471

Wang, S., & Zhu, X. (2022). Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing. *Policing: A Journal of Policy and Practice*, *15*(4), 2329–2340. https://doi.org/10.1093/police/paab059

Ward, P. (2021). Development of a Small Cybersecurity Program at a Community College. *Information Systems Education Journal (ISEDJ)*, *19*(3).

Webster, A., & Gardner, J. (2019). Aligning technology and institutional readiness: The adoption of innovation. *Technology Analysis & Strategic Management*, *31*(10), 1229–1241. https://doi.org/10.1080/09537325.2019.1601694

Weick, K. E. (2005). Organizing and Failures of Imagination. *International Public Management Journal*, *8*(3), 425–438. https://doi.org/10.1080/10967490500439883

Weick, K. E. (2006). The role of imagination in the organizing of knowledge. *European Journal of Information Systems*, *15*(5), 446–452. https://doi.org/10.1057/palgrave.ejis.3000634

Wilczek, E. (2021). Archival Engagements with Wicked Problems. *The American Archivist*, *84*(2), 468–501. https://doi.org/10.17723/0360-9081-84.2.468

Whilst registered as a candidate for the above degree, I have not been registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award.