The Future of Cyber Conflict Studies: Cyber Subcultures and The Road to Interdisciplinarity

Dr. Joe Burton

ABSTRACT

This article has two aims: first, to examine the future of cyber conflict studies and how the study of cyber security can develop in a more interdisciplinary way; second, to assess the meaning of "offensive" and "defensive" cyber security from the perspective of a variety of different academic disciplines. The article argues that a more holistic and nuanced understanding of cyber offence and defence can be achieved if some of the intellectual silos and disagreements that have characterised the debate so far can be deconstructed and overcome. The article is in three parts. The first section briefly outlines some of the definitional fog that has plagued the cyber security discipline, including over what constitutes cyber offense and defence. The paper then summarises four different subcultures of cyber conflict studies that understand and study cyber security in different ways: International Relations (IR), Political Psychology, International Law, and Computer Science. The concluding section discusses how the cyber conflict studies discipline can move forward, be made more rigorous, and less prone to pathology and dead ends, including through the formation of a cohesive but heterogenous epistemic community.

Dr. Joe Burton is an Associate Lecturer in the School of International Relations at the University of St Andrews. Prior to that he was a Marie Curie (MSCA-IF) fellow at Université libre de Bruxelles (ULB) where he worked on the two-year European Commission-funded project Strategic Cultures of Cyber Warfare (CYBERCULT) and a Senior Lecturer in the New Zealand Institute for Security and Crime Science (NZISCS), University of Waikato. Dr Burton has worked at the highest levels of professional politics and policy, as an advisor to Cabinet Ministers in New Zealand and the UK, a national campaign coordinator, legislative assistant, researcher, and political organiser. He is a recipient of the US Department of State SUSI Fellowship. Dr. Burton holds a Doctorate in International Relations and a Master of International Studies from the University of Otago, New Zealand, and an undergraduate degree in International Relations from Aberystwyth University in Wales.

INTRODUCTION

Interdisciplinarity in the study and approach to cyber security has been a regularly stated aim of cyber security researchers and practitioners. Although the immediate and practical protection of computer networks is typically viewed as a job for technical professionals, there are broader social, psychological, political, and legal drivers of cyber conflict and cooperation that are equally important. Despite this being apparent to most in the field, the goal of taking an interdisciplinary approach combining the perspectives of different disciplines, has been a difficult one to achieve. Different lexicons, pedagogies, research methods, and research and policy communities exist. While the emerging discipline of cyber conflict studies has improved its communication and interaction, including at interdisciplinary conferences and through interdisciplinary journals,[1] cyber security research and practice continues to be siloed and at times parochial.

This article seeks to reflect on these problems and explore how the discipline might continue to break down barriers between some of the core research areas in cyber security. In doing so the article presents three core arguments. The first is that spending time trying to understand how offense and defense are perceived in different epistemological communities is an important task, especially as attempts to do so are rare.[2] Knowing the ways colleagues approach their study of cyber security can help avoid some of the pathologies and silos that have characterised the advancement of the discipline to date. Second, drawing on arguments from the security cultures and strategic culture literature, it is argued that each of the disciplines considered in this article—IR, Political Psychology, Law, and Computer Science—constitute distinct subcultures of cyber conflict studies with their own ideas, ordering devices, narratives, framings, and

behaviours. These subcultures, which have their own frictions and synergies, have emerged over many years, and constitute communities of knowing and understanding cyber security that should be better understood. The third argument relates directly to the future of the discipline. In moving forward cyber conflict studies has the potential to become a more cohesive but heterogenous epistemic community that contains a multitude of perspectives which enhance global security and reduce cyber conflict.

1. STUCK IN THE MUD? A SUMMARY AND CRITIQUE OF THE OFFENSE/DEFENSE DEBATE

The study of cyber security sometimes feels like it is stuck in the mud, unable to move forward, and often mired in stale and unresolvable debates. The tendency to adopt binary (i.e., offense/defense) approaches to complex questions of technology and policy is one example. How and when to act defensively or offensively in cyber security is a difficult question that presents normative and ethical implications and can lead to unintended consequences. The tendency to view complex political, social, and technological questions as a binary is not unique to cyber security. In other fields, the dichotomy between "good and evil," "right and wrong," for example, has led to philosophical debates that remain unresolved after centuries. At a technical level, there are many grey areas in cyber security between offense on the one side and defence on the other. The most obvious of these is the idea of "active" cyber defence,[3] which to some is a euphemism for offense by any other name while, to others is a set of technical tools—honeypots, for example—that present opportunities to monitor, retaliate or deploy countermeasures against malicious actors.

The lack of clarity in cyber conflict studies stems not only from the tendency to cast debates and policy options in binary terms but from the uncertainty of the domain and the inherent lack of security that both offensive and defensive postures provide. Defense is acknowledged as extraordinarily difficult due to the nature of the technology itself, its ubiquity, the need to supply cheap (and therefore unsecure) cyber products, and the ever-growing attack surface that computer networks provide. On the offense side, the use and development of offensive tools is underpinned by intractable and ongoing geopolitical disputes. These are exacerbated by dynamics within the international system that make it hard to control the spread of offensive cyber capabilities and their malicious use by state and non-state actors, including the growing commercial market in cyber insecurity driven by criminal groups and security dilemmas between nations driven by fear and mistrust.[4] Managing a domain that is largely owned and managed by the private sector, which allows for anonymity and covertness and which provides an effective means of subversion and sabotage has proved immensely difficult. The character of uncertainty in cyberspace has wide-ranging effects, including generating fear, the overestimation of cyber risks, and temporal lags in responding to cyber-attacks, including attribution.[5] In this environment, acting offensively is no guarantee of a more effective defense, and acting purely defensively is inherently flawed.

Making things worse is the tendency to shoehorn cumulative experiences of insecurity, war, and conflict into the offense/defense debate in ways that are not conducive to peaceful use of ICT or accurate assessment of the present and future of cyber conflict. This occurs through the widespread (mis)use of historical analogies in the field—especially the tendency to link cyber with conventional military operations (cyber pearl harbour) or other security problems, such as terrorism (digital 9/11), and the broader securitization and militarization of the field.[6] It also exists in national approaches to cyber security, where countries appear to be approaching cyber security in ways that are deeply conditioned by past actions (often unsuccessfully). For example, the US approach exhibits particular traits that seem to many observers to be unhelpful to enhancing US cyber security—including the desire to project power internationally by using offensive cyber capabilities, to disrupt and deter non state actors beyond US borders, and an exceptionalism that holds that the US has a unique role as a global leader in cyberspace.[7] In the military sphere in particular, the dominance of Cold War thinking and the application of military concepts to cyberspace has created inherent insecurities, including the belief that having cyber capability is a deterrent, that cyber tools are effective in creating battlefield "effects," and that they are effective means of force amplification multiplicator or indeed force protection.[8] Despite growing scepticism over the utility of cyber as offensive tools,[9] and the blowback effects that have been created by using them,[10] this type of thinking continues to shape the contemporary cyber security debates in sometimes unhelpful ways.

2. SUBCULTURES OF CYBER CONFLICT STUDIES

Approaching the cyber offence debate from the perspective of several different theoretical and disciplinary perspectives is one way to move the debate forward. As argued in this section of the article, each of the key disciplines covered (IR, Political Psychology, Law and Computer Science) offer unique insights into the offense-defense problem, but when combined provide both a better understanding of some of the paradoxes and pathologies in the debate and a path forward to resolving some its intractable difficulties. These disciplines contain unifying ideas and foci that form the basis of distinct subcultures of cyber conflict studies and epistemic communities, defined here as "a network of professionals with recognized expertise and authoritative claims to policy-relevant knowledge in a particular issue area."[11]

International Relations (IR) as an epistemic community

Students and scholars of International Relations are part of a community of knowledge and practice that stretches back to the founding of the discipline after the First World War. This was a conflict of attrition in which a stalemate illustrated that offensive campaigns were not decisive and that defensive measures could create long drawn-out conflicts that inflicted great costs on both sides. The task of IR scholars was to try and address the strategic, ideational, and structural deficiencies and pathologies on which the war was based. During

the Cold War, the discipline's most consuming focus was on managing the perils of nuclear capabilities: how they could be use offensively (and coercively), how to defend against them, and how to find a balance between offense and defense that could provide stability.[12]

Because IR is a community of knowledge and practice that shows significant continuities, in which knowledge accumulates, and in which various path dependencies exist, approaches to understanding cyber strategy have followed a similar direction. Scholars have debated cyber coercion,[13] cyber stability,[14] and the offense-defense balance in cyberspace.[15] While there are nuclear lessons for cyber,[16] there are also fundamental differences between the management of nuclear and cyber threats. Scholars in the field of IR have tended to lean on old adages and the accumulation of historical knowledge in ways that have not advanced the field enough.

While there are clearly some deep cleavages in the IR community about how to study IR, what to study, and different ontological and epistemological assumptions about some of the key concepts (the divide between realism, liberalism and constructivism has been widely documented, for example), the IR subculture is concerned with a common set of problems and ideas. The first is the nature of power and how it is exercised. Cyber power itself has been analyzed and deconstructed, with a variety of metrics and methods used to study and quantify it.[17] A second central and unifying theme that forms the basis of the IR subculture is the notion of explaining both cooperation and conflict under conditions of anarchy.[18] According to realist assumptions, cyber defense and offense are responses to an anarchic international environment in which there are no overriding laws or central authority. The covertness of cyberspace lends itself to offensive actions and makes defensive ones very difficult, and its global scope makes sovereign control over it next to impossible, despite recent calls for digital sovereignty in the EU and elsewhere.[19] Liberal and constructivist scholarship, conversely, has sought to examine the emergence of international cooperation in the cyber domain, including the establishment of new norms, rights, laws, and institutions. Yet progress has been slow, and norms are easily abrogated in a domain that allows for cheating, covert action and plausible deniability.[20]

Critical approaches to IR and security studies have provided further nuance to the field, in part by questioning the nature of power and knowledge in the cyber field, including who it benefits and the political and commercial interests that cyber insecurity serves. Examining the securitisation and militarization of cyberspace[21] and how offensive cyber operations are often hyped and framed as existential threats (the digital Pearl Harbor and 9/11 narratives, for example)[22] has advanced the field, and the impact of cyber operations on human rights, privacy, and human security have all emerged as significant contributions by IR scholars to the cyber security discipline.

(Political) psychology and the human factor in offensive and defensive cyber

Cyber security is not just about technology but about people and their behaviour. This is

the formative premise of a growing literature on the role of psychology and cognitive factors in explaining the interface between technology and the social world. Like IR, psychology is a broad field, but nevertheless contains some core ideas and foci that define it is a subculture and epistemic community within cyber security studies.

Perhaps the closest intersection between cognitive approaches to cyber security and the field of International Relations has been the recognition that some of the concepts IR scholars have been focused on have important cognitive dimensions. The fear created by cyber security discourse and cyber-attacks themselves has been noted by various scholars,[23] and people's perceptions, particularly those of policy and decision makers, have impacted how they have reacted to cyber intrusions.[24] Scholars have also noted the cognitive schemas[25] that exist in policymaking—these are the "mental maps" through which policymakers approach, perceive, and formulate responses to cyber-attacks, and act as an intervening variable between people and the strategic environment in which cyber-attacks take place. These cognitive schemas are distributed culturally and geographically, either in nation-states, or in transnational subcultures, including policy communities, the military, media, and legal community, for example, and contribute to how people in each of these communities react to and comprehend the implications of the inherent uncertainty of the cyber domain.[26]

Psychological approaches to cyber security are necessarily and obviously focused on people, and the "human factor" in cyber security has been a recurring theme and an active research agenda. Monitoring human interaction with computers, including detecting anomalous patterns, has also become an important part of securing modern computer networks, which suggests an obvious convergence between Political Psychology and the established field of Human-Computer Interaction. Understanding under what circumstances human mistakes occur, how a user responds to cyber security events and how aware they are of cyber threats and vulnerabilities are important considerations for organisational (and therefore, national) security.[27]

The manipulation of human targets has also been integral to many modern cyber security breaches. As Hatfield argues, the social engineering concept had its origins in politics (and intelligence studies), thus providing another important link between psychology and political science approaches to security, and is based on the principal of epistemic asymmetry.[28] That is to say, the people (hackers) who manipulate the victims have a higher degree of knowledge about how the platforms work and are able to stretch and alter the behaviour of their targets through deception. This form of technocratic dominance[29] is also key to understanding the evolution of the computer science epistemic community, as detailed in a subsequent section.

Legalism in a legalistic community

Colin Gray noted the existence of subcultures with the US that had an influence on US

strategic doctrine during the Cold War, noting that there was a community of lawyers, in the State Department and elsewhere, to whom the use of force was an anathema.[30] This legalistic community was predisposed to thinking about international affairs in legal terms and in the context of laws, treaties and regulatory mechanisms. In the current cyber security field, legal scholars have coalesced around a set of ideas and approaches to cyber conflict which exhibit an attachment to key ideas. This cyber legalism has had a positive impact on cyber security practice and policy but failed at the international level to bring meaningful advances to cyber security.[31]

The cyber legal subculture has been naturally predisposed to a focus on norms and laws for the obvious policy reason that nations and academia have needed to understand how international law might apply to complex computer networks that are opaque and favour covert action. Cyber commanders in the military sector, for example, have needed to know when a use of a cyber-attack or operation may be illegal. International law has also been driven by operational needs. The Tallinn Manual process has been foremost in the effort to map out how existing international law might apply to cyber conflict during war, and outside of armed conflict.[32 There have also been sustained effort at the UN level to promote and agree on international cyber norms through the OEWG and GGE processes. While these efforts have yielded some progress, there is a growing frustration in the field around the triumphalism surrounding UN level agreements, when nations that are agreeing to be bound by norms are (a) flagrantly violating them from the outset, or (b) failing to implement them.[33] Debates over the potential negotiation of a digital Geneva convention are but one example. Some legal scholars have endorsed the idea that there is no need for a convention to protect civilians against cyber-attacks when the Geneva convention, they argue, already does. Such an approach, however, may limit the emergence of new agreements with greater specificity which encourage buy-in and adherence from states and the tech sector, including more sophisticated and holistic verification and accountability measures.[34]

These challenges are not just practical problems, they are cultural ones, stemming from the culture of legal approaches from western nations in particular.[35] As analysis by Ross reveals, legal culture tends to lean towards the concept of precedent, which is difficult to establish in cyber security because of the unprecedented nature of cyber technologies, but nevertheless is used as a tool by the legal community to stabilize the seemingly chaotic and controllable nature of cyberspace.[36] In these ways, the legal profession's pre-existing ideas, behaviours and practices shape its response to the challenge of securing cyberspace.

Computer science, network defense and offensive cyber

While there is a risk of assigning an identity to the technical cyber security community, which is broad and diverse, there are also some potentially binding characteristics that constitute a more technically-oriented subculture and epistemic community. The first is an attachment to freedom of information and an aversion to processes that create restrictions

to the flow of data. This is a bedrock principle that underpins the development of modern computing. This has obvious implications for cyber offense and defense – offensive measures can be used to liberate information and defensive measures to protect or impede access to information. Tensions between the values associated with a free and open Internet on the one hand and national security requirements on the other are therefore cultural and technical.

Second, the computer science epistemic community is built on valuing technical expertise and skills and the diffusion of that expertise within a technical community. Although the same could be said of other disciplines, the technical and scientific knowledge that forms the basis of advances in software, hardware and networking technology is not widely shared in society and is deemed of particular value. The idea that computers are a complex technology that wider society or indeed the policy making community does not understand is a bedrock notion in this culture. It also forms part of digital knowledge gaps that continue to be problematic across both academic and policy communities.

This feeds into a wider behavioral characteristic of the cyber security technical community that relates to the tools and technology itself and how it is used. Technical experts might be reluctant to acknowledge this point, but widespread in the subculture is the idea that computer technology is designed to be broken, probed, tested, deconstructed, or hacked. By this logic, understanding what makes computers work involves taking them apart or indeed breaking them. There is status in finding bugs (and bounties now paid for them) and a performative element to major breakthroughs in exploits. Of course, much of this process is necessary to test the technology before or after commercial release and ethical hacking and penetration testing has resultantly become a big industry. But it has also encouraged the profusion of knowledge and skills about how to subvert computer networks that has, in some cases, contributed directly to cyber insecurity. Paradoxically, the profusion and advancement of hacking skills for the purposes of defense has created more vulnerabilities and a more widespread skillset that is being adopted and used to hack into computers for malicious reasons. While there is little technical distinction between defensive security testing and offensive hacking, the intent, behaviour, and results of this behaviour is paramount to understanding modern cyber insecurity.

Finally, an integral part of the cyber security technical subculture which directly influences how offense and defense is understood and practiced is a reticence to have the technology regulated or controlled. The idea that underpins the culture is that technology should be democratising, in the sense of being in the hands of the people. Governments should not be involved in controlling the technology and technology itself is often uncontrollable – it is outside of the capacities of policymakers or legislators to bring about meaningful regulation. The widespread use of ransomware technology fuelled by bitcoin, a technology that is difficult to regulate, and the growing market in spyware or surveillance technology are illustrative examples. This has obvious implications for relationships with other subcultures, as

Internet technologies are disruptive to existing power dynamics and particularly the pre-eminence of the state and meanwhile poses distinct and direct challenges to international law.

3. THE FUTURE OF CYBER CONFLICT STUDIES – TOWARDS A SINGLE EPISTEMIC COMMUNITY

One of the challenges of writing an article covering four complex disciplines, each with many and diverse subfields them, is brevity and over-generalization. The principal elements of each of the subcultures presented above are instrumentalist ones that speak to policy-relevant expertise. The salient point here is that a complete picture of cyber conflict can only be gained by understanding the limitations of each discipline and by learning from the others. In designing cyber security education and advancing research in cyber conflict studies, scholars should pay close attention to what other disciplines offer and the limitations of their own field.

In building a more interdisciplinary approach to cyber conflict studies, what obstacles and impediments are there? Can the silos between subcultures be overcome, and could a single cyber security subculture emerge which is based on shared ideas and mutual understanding?

The first problem here is a political and organizational one within academia. The debate about which subjects and disciplines should be given priority, resources, and funding, is contentious and continuing. Debates about cyber security education take place in a context where humanities and social sciences are not always (or often) funded to the same levels as compared with STEM disciplines; there is pressure on social science and humanities to do more technologically/scientifically focused work, and not always the same pressure on technologists to think more broadly about policy, strategy, or even the psychological dimensions highlighted in this piece. Again, this is a cultural problem exacerbated by diverging ideas and perspectives, the creation of insiders and outsiders, and a behavioral failure to create joint programs, centers, degrees, and training. Weston argues, "In a world that is rapidly progressing with new technologies, being 'outside' of STEM is a bit like being driven around in a car while being forced to sit in the back seat."

These problems are present in funding, ranking, and publishing models, too. IR cyber conflict scholars, for example, will generally receive less credit for publications in journals outside their fields than for publishing in the top IR journals. The UK's Research Excellence Framework has only recently introduced guidelines for accurate and fair assessment of interdisciplinary and collaborative research.[37] This problem pervades the organization of universities which are often structured around siloed departments as opposed to research centres and institutes that encourage collaborative research. Some progress is being made here. For example, the UK Centres of Excellence model for cyber security recognizes the interdisciplinary nature of the field. As this article suggests, however, a broader cultural

change will be needed to move the cyber conflict studies field on from some of its limitations and pathologies.

A second obstacle to developing effective multidisciplinary education has to do with research methods and their incorporation into a cohesive whole. The need to blend quantitative approaches with qualitative ones is a challenge and combining the methods of four or more different fields is an even bigger one. As Mulvenon argues, "the field of cyber conflict must sample from a wide variety of methodologies and tools."[38] Relatedly, finding a common language or lexicon across disciplines is a challenge. In the IR discipline deterrence is a military concept closely associated with the Cold War context and nuclear weapons while in law, it is a legal framework; in psychology, it is about changing the thinking of an attacker – and influencing their psychological decision-making processes. Similarly, in the technical sector, policy is mostly understood as organizational policy, for example, restricting use of USB drives in the workplace. In contrast, government officials and IR scholars understand policy to be about the government's overall direction in cyber security—whether to develop offensive cyber capabilities in the military, for example, or institute mandatory reporting of cyber incidents. Finding a common understanding of language in diverse multinational research and policy environments will be difficult even when integral to a more secure cyberspace.

A further challenge is the need to continue to diversify the field. To pose a provocative question: is cyber conflict studies introducing pathologies into analysis because it is largely male, western, and white? IR is undergoing a reckoning with its inherent biases and colonial assumptions increasingly questioned. The debates about the role of race in securitization theory, and the lack of engagement with theory and practice from the global south has been highlighted.[39] The cyber conflict studies field has yet to engage meaningfully with these problems. The lack of gender balance and ethnic diversity in the field is being challenged and addressed by groups like Women in Cyber Security and other initiatives that advance and mentor underrepresented scholars in the field. While commendable, at the present stage this is window dressing for a more deep-rooted problem—that our approach to cyber insecurity contains a larger epistemological and ontological blind spot to diversity issues.

Creating an environment of reciprocity rather than rivalry between disciplines and scholars is a related issue. This article has been deliberately provocative in pointing out some of the pathologies that exist across the disciplines covered. Yet, unless we collaborate with cyber security professionals from outside of our disciplines, these basic differences in understanding or key terms will not be recognized or overcome. A four-way (at least) street between disciplines is needed where computer scientists, for example, learn about politics and policy issues, and IR scholars learn about the technical aspects of computer science. The need to upskill in areas outside of our own immediate disciplines should be mutually invested in and a reciprocal process. Embedding modules/classes/lectures on the technical aspects of cyber security in policy/IR courses and vice versa is an immediate and low-hanging solution to addressing this problem.

Finally, resourcing a multidisciplinary approach in ways that builds a more cohesive discipline will be important. Not all educational institutes will have the resources to do this well. A concern here is that the richest institutions with the most students create the programs that become a benchmark, which in-turn leads to a further stratification of the education system, with a few elite institutions dominating in a particular area. Creating interdisciplinary programs requires leadership, strategic hiring decisions, strategic funding, and sometimes the restructuring of subsidiary programs. Educational cultures can be resistant to change and slow to adapt. Conversely, requiring computer science students to take political science courses, or psychology courses may lead them to sacrifice essential skills they need to cover in their own discipline.[40] Another issue relates to flexibility and heterogeneity. There appears to be merit in developing common approaches to cyber security, but a one-size-fits-all approach may harm some of the cultural diversity that currently exists within the field. Merging or consolidating subcultures could provide beneficial in some ways but maintaining diversity of thought in understanding the future of offense and defense will be critical too. The future of cyber conflict studies thus arguably lies in creating a heterogeneous epistemic community rather than a homogenous one.

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

NOTES

1. The *Journal of Cyber Policy, Journal of Cyber Security,* and *The Cyber Defense Review* are prominent examples.
2. For a notable and commendable example, see J.S. Blair, A.O. Hall, and E. Sobiesk, "Educating Future Multidisciplinary Cybersecurity Teams," in *Computer*, vol. 52, no. 3, pp. 58-66, March 2019, doi: 10.1109/MC.2018.2884190.
3. For a definition of Active Cyber Defense and an exploration of its meaning, see R.S. Dewar, 2014, "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence." *2014 6th International Conference On Cyber Conflict (CyCon 2014), Cyber Conflict (CyCon 2014), 2014 6th International Conference On*, June 7–21, Doi:10.1109/CYCON.2014.6916392.
4. B. Buchanan, 2016, *The cybersecurity dilemma: Hacking, trust, and fear between nations*, Oxford University Press.
5. Monica Kaminska, Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks, *Journal of Cybersecurity*, Volume 7, Issue 1, 2021.
6. See Joe Burton & Clare Lain, 2020, Desecuritising cybersecurity: towards a societal approach, Journal of Cyber Policy, 5:3, 449-470, DOI: 10.1080/23738871.2020.1856903.
7. J. Burton, 2021, 'Defending forward' through 'Persistent Engagement': Assessing the Strategic Cultural Determinants of US Cyber Security Strategy,' Paper presented at BISA US Foreign Policy working group.
8. M. Smeets, 2018, The Strategic Promise of Offensive Cyber Operations, *Strategic Studies Quarterly*, 12(3), 90–113, http://www.jstor.org/stable/26481911.
9. B.Valeriano and R.C. Maness, 2015, *Cyber war versus cyber realities: Cyber conflict in the international system*, Oxford University Press, USA.
10. J. Radack & W. Neuheisel, 2021, SolarWinds Is Not the 'Hack of the Century.' It's Blowback for the NSA's Longtime Dominance of Cyberspace, https://www.commondreams.org/views/2021/01/27/solarwinds-not-hack-century-its-blowback-nsas-longtime-dominance-cyberspace.
11. https://www.britannica.com/topic/epistemic-community.
12. R. Jervis, 1979, Why Nuclear Superiority Doesn't Matter. *Political Science Quarterly*, 94(4), 617–633, https://doi.org/10.2307/2149629.
13. B. Valeriano, B.M. Jensen, and R.C. Maness, 2018, *Cyber Strategy: The Evolving Character of Power and Coercion*, Oxford University Press.
14. F.D. Kramer, 2012, Achieving international cyber stability, *Georgetown Journal of International Affairs,* 121-137.
15. Rebecca Slayton, What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security*, 2017; 41 (3): 72–109. doi: https://doi.org/10.1162/ISEC_a_00267.
16. Joseph S. Nye, Jr., 2011, Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly* 5(4): 18-38.
17. https://www.iiss.org/blogs/-paper/2021/06/cyber-capabilities-national-power.
18. See J. Lindsay, presentation to Hague conference on cyber norms, November 2021.
19. Frances G. Burwell and Kenneth Propp, 2020, The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World? https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf.
20. A. Grigsby, 2017, The end of cyber norms, *Survival,* 59(6), 109-122.
21. J. Burton & C. Lain, 2020, Desecuritising cybersecurity: towards a societal approach, *Journal of Cyber Policy*, 5(3), 449-470.
22. S. Lawson, 2013, Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats, *Journal of Information Technology & Politics*, 10(1), 86-103.
23. M.A. Gomez and E.B. Villar, 2018, Fear, uncertainty, and dread: Cognitive heuristics and cyber threats, *Politics and Governance*, 6(2), 61-72.
24. Ibid.
25. M.A. Gomez, 2021, Overcoming uncertainty in cyberspace: strategic culture and cognitive schemas, *Defence Studies*, [Online] 21 (1), 25–46.
26. Aaron F. Brantly, Risk and uncertainty can be analyzed in cyberspace, *Journal of Cybersecurity*, Volume 7, Issue 1, 2021, tyab001, https://doi.org/10.1093/cybsec/tyab001; M.A. Gomez (2021) Overcoming uncertainty in cyberspace: strategic culture and cognitive schemas, Defence Studies, 21:1, 25-46, DOI: 10.1080/14702436.2020.1851603.

NOTES

27. B.M. Bowen, R. Devarajan, and S. Stolfo, *2011, November. Measuring the human factor of cyber security*, In 2011 IEEE International Conference on Technologies for Homeland Security (HST) (230-235), IEEE.
28. J.M. Hatfield, 2018, Social engineering in cybersecurity: The evolution of a concept, Computers & Security, [Online] 73, 102–113.
29. Ibid, 104.
30. Colin S. Gray, "National Style in Strategy: The American Example." *International Security* 6, no. 2 (1981): 21-47; Colin S. Gray, Nuclear Strategy and National Style (Lanham, Md.: Hamilton Press, 1986), 22.
31. Lucas Kello, Cyber legalism: why it fails and what to do about it, *Journal of Cybersecurity*, Volume 7, Issue 1, 2021, tyab014, https://doi.org/10.1093/cybsec/tyab014.
32. https://ccdcoe.org/research/tallinn-manual/.
33. For a discussion on implementation of cyber norms, see Kerttunen, M. and Tikk, ~E. (2021), Putting Cyber Norms Into Practice: Implementing the UN GGE 2015 recommendations through national strategies and policies, available: https://cybilportal.org/wp-content/uploads/2021/11/Putting-Cyber-Norms-in-Practice.pdf.
34. J. Guay and L. Rudnick, 2017), What the Digital Geneva Convention means for the future of humanitarian action, UNHCR, https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/.
35. R. Ross, 2002, Communications Revolutions and Legal Culture: An Elusive Relationship, *Law & Social Inquiry*, 27(3), 637-684. doi:10.1111/j.1747-4469.2002.tb00822.x.
36. Ibid, 641.
37. Research Excellence Framework, 2021, Interdisciplinary Research, https://www.ref.ac.uk/about/interdisciplinary-research/.
38. J. Mulvenon, 2005, Toward a cyberconflict studies research agenda. IEEE Security & Privacy, 3(4), 52-55.
39. A. Howell and M. Richter-Montpetit, 2020, 'Is securitization theory racist? Civilizationism, methodological whiteness, and antiblack thought in the Copenhagen School,' *Security Dialogue,* 51(1), 3–22, doi: 10.1177/0967010619862921; Amitav Acharya and Barry Buzan, The Making of Global International Relations: Origins and Evolution of IR at Its Centenary, Cambridge University Press, 2019.
40. Fred S. Roberts, The Challenges of Multidisciplinary Education in Computer Science Roberts, *Journal of Computer Science and Technology*, Beijing Vol. 26, Iss. 4, (July 2011): 636-642.