Journal of Strategic Security

Volume 15 | Number 2 Article 3

Strategy in an Uncertain Domain: Threat and Response in Cyberspace

Joe Devanny
King's College London, joseph.devanny@kcl.ac.uk

Luiz Rogerio Franco Goldoni
Brazilian Army Command and General Staff College (ECEME), luizrfgoldoni@gmail.com

Breno Pauli Medeiros
Brazilian Army Command and General Staff College (ECEME), breno.pauli@gmail.com

pp. 34-47

Recommended Citation

Devanny, Joe; Goldoni, Luiz Rogerio Franco; and Medeiros, Breno Pauli. "Strategy in an Uncertain Domain: Threat and Response in Cyberspace." *Journal of Strategic Security* 15, no. 2 (2022) : 34-47.
DOI: https://doi.org/10.5038/1944-0472.15.2.1954
Available at: https://digitalcommons.usf.edu/jss/vol15/iss2/3

Strategy in an Uncertain Domain: Threat and Response in Cyberspace

Abstract

Over the last decade, "cyber power" has become an increasingly prominent concept and instrument of national strategy. This article explores the nature of contemporary cyber power, focusing on how states should respond to "cyber uncertainty." Cases of cyber operations against Estonia, Georgia, and Ukraine, as well as cyber operations conducted (and suffered) by the United States, highlight the evolving role of cyber operations as an instrument of statecraft. Given the complexity of cyber forensics and the polluted information environment of the global public sphere, the public diplomacy of coordinated attribution statements cannot be expected to cut through conclusively or uniformly. States must therefore organise themselves effectively to produce and implement coherent cyber strategy, improving their relational cyber power. This should focus on cyber security and resilience, but also including effective cyber diplomacy, and assessment of what sovereign offensive capabilities are desirable and feasible.

Introduction

Edward Snowden's 2013 revelations about the practices of the U.S. National Security Agency and its allies in the 5 Eyes partnership highlighted the prevalence of digital espionage and the challenges faced by states in improving communications security and protecting digital data.[1] The contemporaneous rise in offensive cyber operations as a tool of state and non-state actors has required greater priority to cyber defence and offense in national strategies. Cyber operations against adversary infrastructure are now an increasingly common part of a state's toolkit, whether the reportedly US-Israeli *Stuxnet* operation against Iranian nuclear infrastructure, or the reportedly Russian cyber operations against targets in Estonia, Georgia, and Ukraine.[2]

A state's cyber power is therefore an increasingly important component of wider national power.[3] It is a relevant dimension in national efforts to enhance socio-economic development and prosperity, information security, national resilience, domestic security and national defence. It is, therefore, a cross-cutting priority in national security strategy.

This article focuses on one aspect of the strategic impact of cyber operations, namely the problem of uncertainty and the challenge of establishing widespread acceptance of attribution. The problem of cyber uncertainty is manifested in a congested grey zone of competition and conflict between state and non-state actors. With asymmetries of knowledge and understanding between state actors and within the global public sphere, uncertainty is a pervasive feature of the cyber domain. The article draws on case study analysis to highlight the challenges that states must address in cyberspace. The article concludes with an assessment of contemporary cyber power and a tentative forecast of future directions for national strategy.

The Congested Grey Zone and Cyber Uncertainty

According to a former senior United Kingdom cyber official: "There have been more than 200 acts popularly portrayed as state-on-state cyber-attacks. Most have been a combination of espionage, media influence, economic coercion, and political intervention, deliberately calibrated below the legal threshold for an act of aggression that would justify an armed response, and therefore in the grey zone between peace and war."[4] The acceleration and intensification of this threat is global, but it is experienced differently depending on the strategic situation of a given state. The most capable state actors have developed offensive cyber capabilities and integrated these into existing defence and intelligence communities, such as U.S. Cyber Command or the United Kingdom's recently avowed National Cyber Force.[5]

Competition and conflict between states manifests a particular character in the cyber domain. However, the nature of inter-state competition and conflict is enduring, channelling the Clausewitzian distinction between the character and nature of war. It is shaped by rival claims and objectives, the fundamentally agonistic feature of which arguably defines the concept of the political.[6] As such, it is unsurprising that the first reported decades of cyber operations can be seen to have followed settled lines of interstate competition and conflict, as well as conforming to the on-going 'global war on terrorism' in the case of coalition cyber operations against Daesh.

The article uses case study analysis to illustrate the problem of cyber uncertainty, focusing on the cyber operations against Estonia in 2007, Georgia in 2008, and Ukraine in 2016. These operations were consistent with the policies pursued overtly by the Russian Federation during on-going bilateral tensions and/or specific periods of armed conflict with the victim states. Even so, the Russian state denied responsibility, shifted blame and tried to spread doubt about the identity of the culprits—signature traits of the "heavily contested information environment" surrounding cyber attribution.[7] Such operations inhabit a congested grey zone of competition and conflict between states and non-state actors.[8] Whether the resultant deniability is widely perceived as plausible or implausible, covert action has long been employed by states to interfere in the affairs of other states; cyber capabilities are merely the latest chapter in this history, amplifying a state's options for covert action.[9] The deeply technical nature of the domain and the complexity of the forensic analysis necessary to determine attribution, creates asymmetries of knowledge and understanding, exacerbating existing fissures between states and across the global public sphere. This additional layer of cyber uncertainty complicates the decisions facing victim states and their allies in how to respond to cyber operations.[10]

DOI: https://doi.org/10.5038/1944-0472.15.2.1954

Uncertainty is exacerbated by states' use of proxies and cut-outs.[11] It is amplified further by possibility of false flag operations and deliberate misdirection. It has been reported that the U.S. Central Intelligence Agency had developed anti-forensics tools, for example by applying non-English language settings (including Russian and Korean) to its malware.[12] Similarly, a Russian intelligence agency reportedly conducted a cyber operation against the 2018 Winter Olympics, unsuccessfully trying to implicate North Korea as the perpetrator.[13] Without the forensic tools possessed by major cyber and intelligence powers such as the United States, or by the most capable threat intelligence companies—and potentially even with such expertise—the attribution of cyber operations can be a difficult, time-consuming process. And given the arcane, exclusive nature of attribution, and the polluted, contested nature of the global information environment, legitimating attribution judgements in the global public sphere is a significant challenge for public diplomacy.

Social, economic, and political life increasingly depends on and is shaped by digital technologies. This is also the case for inter-state competition and conflict: Contesting narratives through digital diplomacy and subversive disinformation operations; the increasingly online activities of intelligence agencies, armed services and aligned non-state actors, achieving effects in and through cyberspace. Contemporary multi-domain operations entail a cyber dimension.[14] And strategically, actors employ cyber operations for compellence and dissuasion, although efficacy is contested.[15] Given the complexity of physical and virtual layers that constitute cyberspace, identifying a cyber operation and attributing it to a specific culprit is an effort requiring different levels of analysis and is likely to rely on cyber forensic equities in both the state and private sectors. Where investigating states possess significant intelligence capabilities, it is possible that human and signals intelligence reporting might contribute to the totality of evidence supporting attribution analysis, providing insights into the technical operational practices of the alleged culprit (state or non-state) actor or into elite decisions authorizing such cyber operations.[16]

Where such sophisticated, composite capabilities for attribution analyses are absent, or else insufficient, attribution is often guided by lower-confidence, *cui bono* logic and/or by the receipt of attribution analyses shared by more cyber-capable states. In the latter case, there is a question of trust potentially exacerbated by information asymmetry: Is attribution assessment shared simply as a global public good, or to further the foreign policy objectives of the sharing state(s)? Following *cui bono* logic in the absence of other information, having explored the relevant geopolitical context, the actor most likely to benefit from the operation might plausibly be regarded as a potential perpetrator.[17] Indeed, unless the cyber operation is purely retributive and destructive, the instrumentality of the operation as a compellent or deterrent action arguably relies on the victim correctly inferring the culprit's true identity and intent.[18] Consequently, it has been observed that cyber operations more often focus on degrading adversary capabilities than on achieving compellence or dissuasion.[19]

Cyber operations against state and non-state targets instrumentalize uncertainty in the pursuit of national (and sometimes simply acquisitive and criminal) objectives. Deniability, however implausible, is particularly important from the perspective of international law and the prospect of being held accountable.[20] The absence of dispositive evidence of a culprit's identity complicates a victim state's decision process, calling into doubt the basis for retaliatory or other responses.

Cyber Operations and Russian National Strategy

Russian state efforts over the last decade to re-assert influence and relevance in global affairs have been described as a case of "asymmetric balancing."[21] The strategy aims to counterbalance adversaries through a range of actions to achieve effects without reaching the threshold of armed conflict with a major adversary. Notable cyber operations in this period that appear to be consistent with such a strategy are those against Estonia in 2007, Georgia in 2008, and Ukraine in 2014, and 2016. The three cases are different, but indicate an evolving method of integrating cyber and conventional capabilities in combined operations.

Between April and May 2007, Estonia was the target of a series of cyber-attacks against its government websites, banking system, internet service providers, telecommunications, and news agencies. There were three waves of attacks in total, ranging from Distributed Denial of Service (DDoS) to digital vandalism. The attacks had a significant effect on Estonia, a country that was already highly interconnected, with considerable digital access to public services. Estonia's digital exposure led its Foreign Minister to claim that the attacks were real, virtual and psychological.[22] The cyber operations against Estonia occurred in the context of growing tensions between Russia and Estonia over the re-location of a statue honoring Soviet soldiers.[23] Tensions escalated into public protests in Tallinn, amplified by Russia's sharp public criticism of the statue's relocation.[24] It was in this suggestive context of sharply deteriorating bilateral relations that the wave of cyber operations was conducted against Estonia.

The cyber operations also occurred in the context of a broader set of coercive or retaliatory actions: An unofficial blockade disrupting cross-border trade with Estonia; domestic political calls for diplomatic and economic sanctions; and attacks against the Estonian embassy in Moscow reportedly by national youth groups, unhindered by local law enforcement. The digital disruptions were conducted against strategic targets, such as financial services, communications hubs, and government websites. The then Estonian defence minister described the totality of the measures as a form of psychological terror.[25]

Attempts to trace the attack suggested that they originated in multiple countries, including Egypt, Peru, and Vietnam.[26] Furthermore, instructions on how to carry out the attacks had been published on the internet, multiplying the hypothetical points of origin of the attacks. Despite these elements of uncertainty, the political context and the operation's scale and level of coordination was suggestive of some degree of Russian state involvement or toleration.[27] Needless to say, Russia has repeatedly rejected this allegation. The re-location of a monument in Tallinn did not pose a significant national security threat to Russia, representing perhaps more of a snub to national pride, particularly when carried out by a smaller neighbor. This suggests cyber operations could have been chosen as a low-cost response, perceived as entailing low risk.[28] The implausible deniability implicit in the cyber operations against Estonia highlighted the potential for states to conduct—or contract proxies to perpetrate—disruptive or destructive operations against adversaries in cyberspace whilst retaining both a consequential degree of uncertainty and a sense of restraint, for example, calibrating offensive operations to test, but not to flagrantly violate, the threshold for triggering the collective defence provision (Article 5) of the North Atlantic Treaty. This ensured that Russia was not subject to significant retaliatory measures following this episode.

The Estonia case should have served as a clear warning to states that improvements were necessary in cyber security practices in the public and private sectors to reduce the risk of being subject to damaging digital disruptions.[29] Unsurprisingly, Estonia acted on this warning. It introduced a range of measures improving national cyber defence and resilience. Estonia created a Cyber Defence League, a defence agency within the military hierarchy, comprising expert volunteers defending Estonia's digital infrastructure. Diplomatically, the North Atlantic Treaty Alliance (NATO) Cooperative Cyber Defence Center of Excellence—in preparation prior to the 2007 attacks—was created in 2008 and located in Tallinn. The Center represents a cyber knowledge-generation and -exchange initiative, improving NATO member states' cyber defence capabilities.

Estonia was not the only state in this period to be subjected to digital disruptions during diplomatic contestation with Russia. In 2008, as the result of tensions arising from the separatist movement in South Ossetia and the country's growing proximity to NATO, the situation in Georgia deteriorated, culminating in a short period of armed conflict with Russia. Russian military operations were accompanied by cyber operations.[30] This represented a relatively new situation, regarded by one scholar as "the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in other warfighting domains."[31]

As with Estonia, cyber operations against Georgia included DDoS attacks and digital vandalism against government websites, communication agencies, internet providers and the Georgian media. Georgia's financial and transport infrastructure were targeted. Instructions for conducting DDoS attacks against Georgian servers had also been disseminated publicly, again illustrating an effort to empower proxies and/or shift blame. Georgia's case differs from Estonia, however, due to the increased sophistication and coordination of the operations. One of the first sites to be taken down was a forum of Georgian hackers, to prevent attempts to re-establish interrupted services or to retaliate in cyberspace.[32] Following the disruption of Georgia's communications infrastructure, Russian invaded with conventional armed forces. Analysis of the Georgia case has led some to argue that the extent of operational coordination implies the systematic integration of cyber domain operations with those of traditional forces at the strategic, operational, and tactical levels.[33] Whatever the efforts to obscure ultimate responsibility for the cyber operations, the director of Georgia's National Security Council argued that, in the context of armed conflict, Russian denials of responsibility were implausible.[34]

The Georgia case highlights the combination of implausibly denied cyber operations with avowed conventional military operations. On the ladder of uncertainty, the next logical step would be to align implausibly deniable cyber operations with implausibly deniable military operations, for example by creating uncertainty about command and control over units fighting in an adversary's territory. Just six years later, this would become a salient feature of Russian operations against Ukraine from 2014 to present.

Prior to the 2014 invasion of Ukraine by Russia, bilateral diplomatic tensions had intensified in 2013 over Ukraine's negotiations with the European Union and Russian fears that Ukraine was moving outside of its sphere of influence.[35] This prompted the operation to annex Crimea, with a hastily convened referendum to declare that a majority of the population voted to be incorporated into the Russian Federation.[36] Annexation of Crimea and continued destabilization of eastern Ukraine prompted a diplomatic response from the European Union and United States, in the form of coercive economic measures, without altering de facto Russian control of Crimea or on-going instability in eastern Ukraine.[37]

The cyber dimension of the attack on Ukraine involved efforts to destabilize the Ukraine government and create a climate of confusion and uncertainty between government and society, using digital disinformation operations including the production and dissemination of "fake news".[38] In addition, the persistence of cyber operations undermined the effectiveness of communication between Ukraine's government and armed forces.[39] The range of operations spanned information operations, with DDoS attacks against strategic websites; leaking government and private data; and messages sent to Ukraine military personnel to encourage desertion. Cyber operations were also conducted against Ukraine's energy infrastructure, resulting in a power blackout in Kiev.[40] Several Western states subsequently publicly attributed the blackout to Russian action.[41] Even so, global perceptions of Russia's culpability for cyber operations against Ukraine since 2014 have arguably come more from the political context than from widespread knowledge, understanding or acceptance of dispositive evidence of attribution.[42]

The Ukraine case introduces a significant element of the strategic debate about offensive cyber operations: The targeting of civilian infrastructure. As states develop offensive cyber capabilities, they are faced with consequential ethical and strategic decisions about how and when these capabilities should be used.[43] Offensive cyber operations can be used tactically or operationally, integrated in multi-domain operations, but the strategic targeting of critical infrastructure increases the risk that cyber operations lead to escalation out of the grey zone and into armed conflict. This is a particular risk given the confusion in public debate between incidents of cyber espionage and offensive cyber operations—both being labelled as cyber attacks requiring cost-imposition—that was discernible in the wake of the SolarWinds breach.[44] In the current environment, in which nation states possess a monopoly on the most sophisticated offensive cyber operational capabilities, the greater the degree of sophistication and alignment with operations in other domains that a given cyber operation required, the stronger will be the implicit assumption that such operations involved some form of state activity or direction, even if dispositive evidence of ultimate responsibility is unavailable.[45]

It is clear from these brief case studies that states are increasingly at risk from sophisticated cyber operations whether conducted in isolation or as part of a coordinated, multi-domain military operation. Both the range of techniques and the degree of integration with other domains appears to have improved during the 2000s. Recent tensions between Iran and the United States, and between Iran and Israel, have seen the reported use of cyber operations as part of carefully calibrated responses designed to control the potential for escalating conflict.[46]

As this section has aimed to demonstrate, a global and public debate is necessary to consider the strategic, institutional, and operational lessons that states should learn from contemporary developments in cyber operations and their role in international relations. Such a debate has developed over the last decade, but is uneven and largely dominated by U.S. voices and issues. This is unsurprising, given the weight of U.S. cyber power, but it risks the distortive impact of assuming that the threats and opportunities of offensive cyber operations affect all states equally. There is a need for a wider global conversation, one that is sensitive to the contingencies and modalities of cyber security in different national and regional contexts.[47]

Conclusion

The cases of Estonia, Georgia, and Ukraine highlight the role of offensive cyber operations in contemporary competition and conflict between states. Given the global nature of the domain, few if any states can prudently ignore the need to cultivate cyber security and resilience. Nor can states simply focus on cyber threats emanating from neighbors or the immediate region. State actors and cybercriminals have global reach. The precise institutional configuration of cyber responsibilities in a state will depend on contingent factors, such as the historical development of sovereign cyber capabilities (whether in the military or civilian intelligence agencies), and the extent to which armed forces have adopted domestic security missions as part of national defence. Whatever the impact of contingency and national specificity, however, some uniform observations are possible.

National strategic decision makers must recognize that military actions in traditional domains now occur increasingly in conjunction with different levels of cyber operations. What happened in Georgia in 2008 and to a greater extent in Ukraine from 2014-onward demonstrates the evolution of cyber operations, as a tool of statecraft and as a military instrument, complementing operations in other domains. The task of contemporary national defence must involve the security and resilience of digital infrastructure. This requires a coherently managed, strategic approach to cooperation between defence, law enforcement and the management of critical infrastructure. The resilience of the digital homeland is now an integral component of national defence. In early 2022, at the beginning of the most recent phase of the Russian invasion of Ukraine, cyber operations appear to have played a less prominent role in wider Russian strategy than might have been anticipated. It is too soon to assess at time of writing (early March) what factors most accounted for this: improved Ukrainian cyber defences; assistance by foreign state and corporate actors; intentional Russian planning that placed lower emphasis on the supporting role of cyber operations; or another contingency that undermined the alignment between cyber and wider operations. Far from undermining the argument that digital resilience is an integral element in national strategy, this latest cyber element of the conflict arguably reinforces the case for states to pursue broad efforts to improve national cyber defences.[48]

The grey zone of uncertainty—however implausible the deniability—exploited by cyber operations requires a national response that transcends improvements in the security of digital targets. States must consider how to reduce uncertainty by increasing national capabilities in cyber forensics. This should not be construed narrowly to refer simply to the creation of a national cyber defence or security center, but broadly to encompass different elements of national power and the role they play in enhancing national cyber forensic capabilities. This list should include: Efforts to build private sector capabilities in cyber security; structured and targeted state intervention in national education to ensure a future pipeline of suitably qualified cyber professionals; and reviewing the contribution of the collection and analysis capabilities of national intelligence agencies to the process of cyber investigation and attribution analysis.

Third, in the same way that national cyber strategy is not solely governmental and involves the crucial contribution of the private sector and wider society in upholding high standards of cyber security, so too does it transcend the domestic to include international and multilateral dimensions.[49] A state's international relations are a major determining factor in identifying its likely cyber adversaries. Recent efforts by Ukraine's and Georgia's allies to publicly attribute cyber operations to Russia are examples of diplomatic solidarity through coordinated public attribution, although the strategy of public attribution is difficult to implement successfully.[50]

Recognition of the need for multi-domain operations is clearly part of a state's response to the rising salience of cyber operations, as is heightened awareness of and response to the cyber risk to defence platforms, command and control and communications infrastructure. Another dimension of the cyber defence conundrum is the issue of the national requirement for an offensive cyber capability. Again, this question is inseparable from questions about the extent to which states can rely on private sector and foreign governmental partners to help to grow its sovereign cyber industrial base. Just as deficiency in national cyber investigation and attribution analysis leaves states reliant on the public good of analyses shared by other states or the services provided by leading cyber security companies, perceived deficiency in a state's ability to respond symmetrically to a cyber operation might reduce the credibility of its overall deterrence strategy, or force it to rely disproportionately on other means. Offensive cyber capabilities should, therefore, increasingly feature in states' national cyber defence strategies.

The above is by no means exhaustive and is necessarily brief as a summary of possible institutional and strategic reforms open to many states in their approach to the problems of cyber uncertainty. Given cyberspace's ubiquity, states need a cyber strategy that encompasses coherently the overlapping issues of cyber defence, cyber security, resilience, and offensive cyber. Most importantly, such a strategic approach should recognize the shaping effects exerted on national cyber strategy by a state's wider national security strategy and foreign policy posture. Cyber operations are only one dimension of a challenge that transcends any one military domain, institutional division within government, boundaries between public and private sectors, and indeed between national governments.

Endnotes

[1] Shane Harris, *@ War: The Rise of the Military-internet Complex* (New York: Houghton Mifflin Harcourt, 2014); Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (London: Guardian Faber Publishing, 2014).

[2] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012); Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Anchor, 2020).

[3] Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Daniel Cassidy, and Anina Schwarzenbach, *National Cyber Power Index 2020: Methodology and Analytical Considerations*. Belfer Center China Cyber Policy Initiative, 2020. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

[4] Marcus Willett, "Assessing Cyber Power," *Survival* 61, no.1 (2019): 85-90, https://doi.org/10.1080/00396338.2019.1569895.

[5] Joe Devanny, Andrew Dwyer, Amy Ertan, and Tim Stevens, *The National Cyber Force that Britain Needs?* King's College London, 2021, https://www.kcl.ac.uk/policy-institute/assets/the-national-cyber-force-that-britain-needs.pdf

[6] Carl Schmitt, *The Concept of the Political* (Chicago: 1996): 46-49.

[7] Florian J. Egloff, "Contested public attributions of cyber incidents and the role of academia," *Contemporary Security Policy* 41, no.1 (2020): 55-81, https://doi.org/10.1080/13523260.2019.1677324.

[8] John Raine, "War or Peace? Understanding the Grey Zone," *International Institute of Strategic Studies* (blog)*,* April 3 (2019), https://www.iiss.org/blogs/analysis/2019/04/understanding-the-grey-zone.

[9] Rory Cormac and Richard J. Aldrich, "Grey is the new black: covert action and implausible deniability," *International Affairs* 94, no.3 (2018): 477-494, https://doi.org/10.1093/ia/iiy067.

[10] Breno Pauli Medeiros and Luiz Rogério Franco Goldoni, "The Fundamental Conceptual Trinity of Cyberspace," *Contexto Internacional* 42, no.1 (2020): 31-54, https://doi.org/10.1590/s0102-8529.2019420100002.

[11] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge: Cambridge University Press, 2018).

[12] Matt Burgess, "WikiLeaks Drops 'Grasshopper' Documents, Part Four of Its CIA Vault 7 Files," *WIRED UK*, July 5, 2017. https://www.wired.co.uk/article/cia-files-wikileaks-vault-7.

[13] Andy Greenberg, "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History," *Wired*, October 17, 2019. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/.

[14] Robert "Jake" Bebber, "Cyber power and cyber effectiveness: An analytic framework," *Comparative Strategy 36*, no.5 (2017): 426-436. https://doi.org/10.1080/01495933.2017.1379833.

[15] Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford: Oxford University Press, 2018).

[16] Herb Lin, "Attribution of Malicious Cyber Incidents," *National Security, Technology, and Law* (2016). https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.

[17] Myriam Dunn Cavelty, "The normalization of cyber-international relations," in *Strategic Trends 2015*: 81-98. ETH Zurich, Center for Security Studies, 2015. https://css.ethz.ch/en/publications/strategic-trends/details.html?id=/t/h/e/n/the_normalization_of_cyberinternational.

[18] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 2008).

[19] Valeriano, Jensen, and Maness, *Cyber Strategy: The Evolving Character of Power and Coercion*.

[20] Jeffrey Hunker, Bob Hutchinson, and Jonathan Margulies, "Role and challenges for sufficient cyber-attack attribution," *Institute for Information Infrastructure Protection* (2008): 5-10. http://www.scis.nova.edu/%7Ecannady/ARES/hunker.pdf; Ruth W. Grant, and Robert O. Keohane, "Accountability and abuses of power in world politics," *American Political Science Review* (2005): 29-43.http://www.journals.cambridge.org/abstract_S0003055405051476.

[21] John Arquilla, Anna Borshchevskaya, Belinda Bragg, Pavel Devyatkin, Adam Dyet, R. Evan Ellis, Daniel J. Flynn et al. *Russian Strategic Intentions* (Naval Postgraduate School: 2019), https://calhoun.nps.edu/handle/10945/62483.

[22] Joshua Davis, "Hackers take down the most wired country in Europe," *Wired magazine* 15, no.9 (2007): 15-09, https://www.wired.com/2007/08/ff-estonia/.

[23] Mark Landler and John Markoff, "Digital fears emerge after data siege in Estonia," *The New York Times,* May 29 (2007), https://www.nytimes.com/2007/05/29/technology/29estonia.html?searchResultPosition=1.

[24] Rain Ottis, "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective," in *Proceedings of the 7th European Conference on Information Warfare (2008)*: 163, https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/.

[25] Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare (1rev)* (Arlington: Center for Naval Analyses, 2017), https://apps.dtic.mil/sti/pdfs/AD1032208.pdf, 11.

[26] Joshua Davis, "Hackers take down the most wired country in Europe."

[27] Stephen Herzog, "Revisiting the Estonian cyber attacks: Digital threats and multinational responses," *Journal of Strategic Security* 4, no.2 (2011): 49-60, https://www.jstor.org/stable/26463926.

[28] Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare*.

[29] Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," *International Journal of Cyber Warfare and Terrorism (IJCWT)* 1, no.1 (2011): 24-34, http://doi.org/10.4018/ijcwt.2011010103.

[30] John Markoff, "Before the gunfire, cyberattacks," *New York Times*, August 13 (2008): 27-28. https://www.nytimes.com/2008/08/13/technology/13cyber.html.

[31] David Hollis, "Cyberwar case study: Georgia 2008," *Small Wars Journal* (Blog), January 6 (2011), 2, https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf.

[32] Paulo Shakarian, "The 2008 Russian cyber campaign against Georgia," *Military review 91*, no.6 (2011): 63. https://www.proquest.com/trade-journals/2008-russian-cyber-campaign-against-georgia/docview/910124995/se-2?accountid=201395.

[33] David Hollis, "Cyberwar case study: Georgia 2008," 8.

[34] Noah Shachtman, "Top Georgian official: Moscow cyber attacked us–we just can't prove it," *Wired Magazine,* March 11 (2009), https://www.wired.com/2009/03/georgia-blames/.

[35] Joe Devanny, "UK National Security Decision-Making in Context: The Ukraine Crisis and NATO's Warsaw Summit Meeting," *Sasakawa Peace Foundation* (2018), https://www.spf.org/projects/upload/UK%20National%20Security%20Decision-Making%20in%20Context%20%28Devanny%29.pdf.

[36] Marie Baezner, *Cyber and Information warfare in the Ukrainian conflict*, no.1, ETH Zurich (2018), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf.

[37]Andrew Foxall, "Putin's cyberwar: Russia's statecraft in the fifth domain," *Russia Studies Centre, Policy Paper* 16 (2016), http://henryjacksonsociety.org/wp-content/uploads/2018/06/Putins-Cyberwar.pdf.

[38] Irina Khaldarova and Mervi Pantti, "Fake news: The narrative battle over the Ukrainian conflict," *Journalism practice* 10, no.7 (2016): 891-901, https://doi.org/10.1080/17512786.2016.1163237.

[39] Michael Connell and Sarah Vogler, *Russia's approach to cyber warfare, 19-23*.

[40] Mark Galeotti, "Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?" *Small Wars & Insurgencies* 27, no.2 (2016): 282-301, https://doi.org/10.1080/09592318.2015.1129170.

[41] David E. Sanger and Steven Erlanger. "Suspicion falls on Russia as 'snake' cyberattacks target Ukraine's government." *New York Times,* March 9 (2014). https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html/; Andrew E. Kramer and Andrew Higgins, "In Ukraine, a malware expert who could blow the whistle on Russian hacking," *The New York Times*, August 16 (2017), https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html/; Andrew Roth and Ellen Nakashima, "Massive Cyberattack Hits Europe with Widespread Ransom Demands," *The Washington Post*, June 27 (2017). https://www.washingtonpost.com/world/europe/ukraines-government-key-infrastructure-hit-in-massive-cyberattack/2017/06/27/7d22c7dc-5b40-11e7-9fc6-c7ef4bc58d13_story.html?utm_term=.6f52ad40e788%2F.

[42] Jessikka Aro, "The cyberspace war: propaganda and trolling as warfare tools," *European View* 15, no.1 (2016): 121-132, https://doi.org/10.1007%2Fs12290-016-0395-5.

[43] Joe Devanny, "The Ethics of Offensive Cyber Operations," *Foreign Policy Centre,* December 3 (2020), https://fpc.org.uk/the-ethics-of-offensive-cyber-operations/.

[44] Joe Devanny, "'Madman Theory' or 'Persistent Engagement'? The Coherence of US Cyber Strategy under Trump," *Journal of Applied Security Research* (2021), DOI: 10.1080/19361610.2021.1872359; Joe Devanny, Ciaran Martin and Tim

Stevens, “On the strategic consequences of digital espionage,” *Journal of Cyber Policy 6*, no.3 (2021), 429-450, DOI: 10.1080/23738871.2021.2000628.

[45] Stephen Blank, "Cyber war and information war a la russe," *Understanding Cyber Conflict: Fourteen Analogies* (2017): 1-18, https://carnegieendowment.org/2017/10/16/cyber-war-and-information-war-la-russe-pub-73399.

[46] Ellen Nakashima, "Trump approved cyber-strikes against Iran’s missile systems," *Washington Post*, June 22 (2019), https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html; Gil Baram and Kevjn Lim, “Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks,” Foreign Policy, June 5 (2020), https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.

[47] Joe Devanny and Tim Stevens, “What Will Britain’s New Cyber Force Actually Do?” *War on the Rocks*, May 26 (2021), https://warontherocks.com/2021/05/what-will-britains-new-cyber-force-actually-do/.

[48] Ciaran Martin, “Cyber Realism in a Time of War,” Lawfare (Blog), March 2 (2022), https://www.lawfareblog.com/cyber-realism-time-war; Joe Slowik, “Contextualizing Cyber Components in Conventional Conflict,” Pylos (Blog), February 25 (2022), https://pylos.co/2022/02/25/contextualizing-cyber-components-in-conventional-conflict/; David E. Sanger, Julian E. Barnes, and Kate Conger, "As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered The War,” The New York Times, February 28 (2022), https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html.

[49] Lucas Kello, *The Virtual Weapon and International Order* (New Haven: Yale University Press, 2019).

[50] Florian J. Egloff and Max Smeets, “Publicly attributing cyber attacks: a framework,” *Journal of Strategic Studies* (2021), DOI: 10.1080/01402390.2021.1895117.