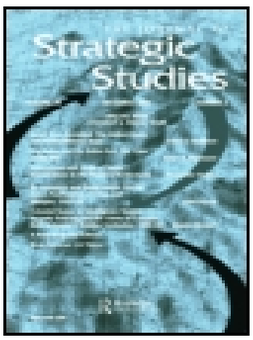

Routledge
Taylor & Francis Group

Journal of Strategic Studies

ISSN: 0140-2390 (Print) 1743-937X (Online) Journal homepage: http://www.tandfonline.com/loi/fjss20

Fancy bears and digital trolls: Cyber strategy with a Russian twist

Benjamin Jensen, Brandon Valeriano & Ryan Maness

To cite this article: Benjamin Jensen, Brandon Valeriano & Ryan Maness (2019): Fancy bears and digital trolls: Cyber strategy with a Russian twist, Journal of Strategic Studies, DOI: 10.1080/01402390.2018.1559152

To link to this article: https://doi.org/10.1080/01402390.2018.1559152

THE JOURNAL OF STRATEGIC STUDIES
https://doi.org/10.1080/01402390.2018.1559152

Routledge
Taylor & Francis Group

ARTICLE

Fancy bears and digital trolls: Cyber strategy with a Russian twist

Benjamin Jensen[a,b], Brandon Valeriano[b] and Ryan Maness[c]

[a]Marine Corps University, Quantico, VA, USA; [b]School of International Service, American University, Washington, DC, USA; [c]Naval Postgraduate School, Monterey, CA, USA

ABSTRACT

How states employ coercion to achieve a position of advantage relative to their rivals is changing. Cyber operations have become a modern manifestation of political warfare. This paper provides a portrait of how a leading cyber actor, Russia, uses the digital domain to disrupt, spy, and degrade. The case illustrates the changing character of power and coercion in the twenty-first century. As a contribution to this special issue on twenty-first century military strategy, the findings suggest new forms of competition short of war.

KEYWORDS Cyber security; coercion; strategy; Russia

In October 2017, major social media firms including Facebook revealed that targeted Russian propaganda during the 2016 US presidential election may have reached as many as 126 million users.[1] These ads, tailored to "unleash the protest potential of the population"[2] formed a new front in a long-term competitive strategy designed to undermine US institutions and resolve. This information warfare campaign, combining propaganda with cyber intrusions, reflects a twenty-first century form of political warfare.[3]

The power to hurt has become the power to hurt online.[4] Just as the nuclear age heralded important changes to conceptualizing the use of force to achieve political objectives, the connectivity of the twenty-first century alters how rival states seek a position of relative advantage and coerce their

CONTACT Benjamin Jensen jensen@american.edu School of International Service, American University, 4400 Massachusetts Avenue NW, Washington, DC 20016, USA

[1]Mike Isaac and Daisuke Wakabayashi, 'Russian Influence Reached 126 Million Through Facebook Alone', *New York Times*, 30 Oct. 2017.

[2]Gerasimov, 'The Value of Science in Prediction', *Military-Industrial Kurier* (27 Feb. 2013).

[3]George F. Kennan on Organizing Political Warfare, 'History and Public Policy Program Digital Archive, Obtained and contributed to CWIHP by A. Ross Johnson', Cited in his book *Radio Free Europe and Radio Liberty*, Ch1 n4 – NARA release courtesy of Douglas Selvage. Redacted final draft of a memorandum dated 4 May 1948, and published with additional redactions as document 269, FRUS, Emergence of the Intelligence Establishment, 30 Apr. 1948.

[4]Erik Gartzke and Jon R. Lindsay, 'Coercion through the Cyberspace: The Stability-Instability Paradox Revisited', in Kelly Greenhill and Peter Krause (eds.), *The Power to Hurt in the Modern World* (Oxford: Oxford University Press 2017).

adversaries. Coercion, the exploitation of potential force short of war,[5] is reborn as disruptive website defacements and denial of service attacks, massive espionage campaigns, deception, and covert psychological warfare designed to shape decisions in rival states.[6]

This paper investigates how Russia employs cyber ways and means to achieve strategic ends. As a contribution to this special issue on twenty-first century military strategy, the paper explores how rival states employ cyberspace to achieve a relative position of advantage and shape their opponents' decision architecture. The Kremlin is not alone in employing cyber coercive instruments as part of long-term competition between rivals. Great powers use any means at their disposal to advance their interests. The US and Israel show a penchant for combining cyber sabotage alongside the threat of military force and other coercive diplomatic instruments.[7] China illustrates how espionage and deception alter the long-term balance of information in incidents such as the Office of Personnel Management intrusion and large-scale intellectual property theft.[8] Even regional actors such as North Korea show how cyberspace can be used to coerce firms, illicitly access hard currency, and spy on rivals.[9] Here, we offer a portrait of one of the leading cyber actors, Russia, and how it employs a mix of coercion and espionage to advance their its interests online.

Cyber strategy has come of age. Strategy is a dialectic of opposing wills that revolves around a set of ideas about how to employ instruments of power to advance a defined objective.[10] Strategy therefore is the "art of creating power."[11] For Robert Osgood, this art of power "must be understood as nothing less than all plans for utilizing the capacity for armed coercion – in conjunction with the economic, diplomatic, and psychological instruments of power – to support foreign policy most effectively by overt, covert, and tacit means."[12] Strategy therefore is a guide to long-term competition and this struggle, by definition, involves interdependent decisions and expectations about rival behavior.[13]

[5]Thomas Schelling, *Strategy of Conflict* (Cambridge: Harvard University Press 1960), 9.
[6]Brandon Valeriano, Benjamin Jensen, and Ryan Maness, *Cyber Strategy: The Changing Character of Cyber Power and Coercion* (New York: Oxford University Press 2018).
[7]On Stuxnet, see Jon R. Lindsay, 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* 22/3 (2013), 365–404; Rebecca Slayton, 'What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessments', *International Security* 41/3 (2016), 72–109.
[8]Jon R. Lindsay, 'The Impact of China on Cybersecurity: Fiction and Friction', *International Security* 39/3 (2014), 7–47.
[9]On the Sony Pictures Hack, see Travis Sharp, 'Theorizing Cyber Coercion: The 2014 North Korea Operation against Sony', *Journal of Strategic Studies* 40/7 (2017), 898–926. For an extensive overview of a known APT linked to North Korea, see Kaspersky Labs, *Lazarus Under the Hood* (25 Nov. 2017).
[10]The idea of strategy as a dialectic come from Andre Beaufre, *An Introduction of Strategy* (London: Faber and Faber 1965 R.H. Barry translation), 22.
[11]Lawrence Freedman, 'Strategic Studies and the Problem of Power', in Thomas Mahnken and Joseph A. Maiolo (eds.), *Strategic Studies: A Reader* (New York: Routledge 2008), 31.
[12]Robert Osgood, *The Entangling Alliance* (Chicago: University of Chicago Press 1962).
[13]Schelling, *Strategy of Conflict*, 3.

In Clauswitzean terms, strategy, as the art of creating power, has an enduring nature and a changing character. The enduring feature is the competitive struggle against an adversary using all available means directed against an, ideally, clear political objective. The changing character resides in the prevailing theories of victory and available resources actors can use to achieve a position of advantage.[14] From political institutions to new technology and changing social norms, interconnected factors define strategic practice.[15] As more and more of our daily lives occur in a digital space, the logic of strategy shifts to a new domain.

To investigate how Russia employs cyber strategy in pursuit of political objectives, this paper proceeds as follows. First, we situate cyber strategy within the broader theoretical literature on coercion and covert signaling. Second, we review documented cyber operations pursued by Moscow. These operations show that most cyber intrusions focus on disruption and harassment alongside espionage required to gain access and collect intelligence. Although Russia has employed cyber instruments alongside major combat operations in Georgia and Ukraine, the preponderance of Russia activity is disruptive rather than degrading. The paper concludes by noting that although Russian cyber information operations are concerning, their efficacy is questionable and these operations represent the actions and declining power.

The character of cyber strategy

Most cyber intrusions between great powers and rival states do not involve wartime exchanges.[16] Rather, they take place in what defense pundits are increasing calling a gray zone short of war. In this respect, the use of cyber operations, defined as the use of malicious code to alter or destroy information or physical networks, is similar to covert action. They reflect concealed means to achieve a political end.

Rival states seek to compel one another and manage escalation risks through a variety of instruments in the shadows. From Sun Tzu and Kautilya to Thomas Schelling and Alexander George, covert action and coercion are major themes in strategic and military theory. As a form of hostile covert action, cyber operations can represent ambiguous signals designed to probe adversary intentions and manage escalation risk. The reality is that cyber operations do not produce concessions in isolation. Instead, they often seek to distract an opponent or amplify a propaganda theme. Furthermore, most cyber operations

[14]On theories of victory, see Benjamin Jensen, *Forging the Sword: Doctrinal Change in the U.S. Army* (Palo Alto: Stanford University Press 2016).
[15]Beatrice Heuser, *The Evolution of Strategy: Thinking War from Antiquity to the Present* (New York: Cambridge University Press 2010), 19–24.
[16]For empirical data on rival state use of cyber, see Valeriano, Jensen and Maness, *Cyber Strategy*.

involve espionage and shaping activities required to understand adversary networks and gain access. The traditional understanding of coercion, as articulated by Thomas Schelling, finds resonance in cyber operations, but only with weak effects.[17] Compellence is rare, deterrence uncertain in a realm of covert action.

Cyber operations, in addition to their latent intelligence value, can act as additive measures that amplify existing strategic signals. Their coercive effect, at least to date, is more latent than manifest due to issues associated with attribution and credibility issues. In a crisis, states can also face problems clearly communicating their intent through signals. This challenge is amplified in cyberspace, where "the linkages between intent, effect, and perception are loose."[18] This dynamic creates a condition in which signals "can be as or more ambiguous when they take place or refer to events in cyberspace than they are when limited to the physical world."[19] There are also unique signaling challenges associated with cyber coercion that limit its power to hurt. According to Borghard and Lonergan, "signaling in cyber space is the problematic of all domains (land, sea, air, space and cyber) because the signal may go unrealized. In other words, in cyberspace only the initiator may perceive the engagement."[20] Similarly, for Gartzke and Lindsay,

> The biggest obstacle to cyber coercion is the difficulty of credibly signaling about potential harm that depends on secrecy to be harmful… Sacrifice of anonymity on which offensive deception depends exposes the cyber attacker to retaliation. Coercive cyber threats thus tend to be more generalized, which undercuts their effectiveness in targeted or crisis situations.[21]

As concealed means, cyber operations sacrifice signal strength for network access but gain benefits from anonymity.

If strategy is a concept concerning how to influence rivals in pursuit of political objectives, then what forms of interaction help states create the power to do so in the digital domain? We propose three distinct strategic logics in cyberspace: disruption, espionage, and degradation.[22] These logics build on earlier work on coercive and coercion as well as recent explorations of cyber coercion, but with an important caveat.[23] Cyber strategy need not seek a direct concession and tends to occur predominantly in the covert, as opposed to overt, space. Rival states use indirect cyber instruments to shape long-term competition more than they seek immediate concessions. Russia

[17]Schelling, *Strategy of Conflict*.
[18]Martin Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica: Rand Corporation 2012), xvi.
[19]Libicki, *Crisis and Escalation in Cyberspace*, xv.
[20]Erica Borghard and Shawn Lonergan, 'The Logic of Coercion in Cyberspace', *Security Studies* 26/3 (2017), 452–481.
[21]Gartzke and Lindsay, 'Coercion through the Cyberspace', 26.
[22]Valeriano, Jensen, Maness, *Cyber Strategy*.
[23]On coercive diplomacy, coercion, and cyber coercion as they relate to one another, see Valeriano, Jensen and Maness, *Cyber Strategy*.

utilizes destabilizing hacks to harass targets toward bending to Moscow's will. As a coercive tool available to states, cyber operations therefore represent a weak form of coercive diplomacy. Digital intrusions are meant to be used with other sticks and carrots to shape an adversary's decision-making.

Cyber disruptions are a low-cost, low-payoff form of cyber strategy designed to shape the larger bargaining context. These cheap signals likely do not achieve sufficient leverage to compel a target.[24] Rather, they seek to probe an adversary: testing their resolve, signaling escalation risk, and supporting larger propaganda efforts. Website defacements and distributed denial of service (DDoS) incidents are a form of tacit bargaining. According to George Downs and David Rocke, "tacit bargaining takes place whenever a state attempts to influence the policy choices of another state through behavior, rather than by relying on formal or informal diplomatic exchanges [alone]."[25] Low-cost cyber disruptions pressure a rival, through either signaling the risk of crisis escalation or, in combination with propaganda efforts, undermining public confidence in existing policy preferences. Website defacements often echo particular narratives designed to limit policy options for a rival, portraying the opposition as extreme versions of evil, for example how website defacements characterize the Ukrainian government as fascists or Nazis.

As a strategy, cyber espionage concerns altering the balance of information to achieve a position of advantage. Activities can range from simple network penetration to retrieve information to manipulating data to corrupt a rival's confidence in their own systems. These actions are not coercive in the traditional sense. Rather, they concern long-term competition and how rival states seek to find ways of exploiting information asymmetries. Espionage represents efforts to steal critical information or manipulate information asymmetries in a manner that produces bargaining benefits between rival states engaged in long-term competition.

Cyber degradation – coercive operations designed to sabotage the enemy target's networks, operations or systems – is more likely to have a compellent effect than disruptions or espionage. Yet, this effect is rare because many times the target is hardened or too complex to be knocked out for extended periods as a result of malicious cyber actions. This form of cyber strategy resembles denial coercion used in airpower and tends to exhibit sunk costs due to its complexity and tailored design (optimized for a specific system and to achieve destructive effects).[26] This high-cost, high-payoff dynamic makes

[24]James D. Fearon, 'Rationalist Expectations for War', *International Organization* 49/3 (1995), 379–414; James D. Fearon 'Signaling Foreign Policy Interests Tying Hands versus Sinking Costs', *Journal of Conflict Resolution* 41/1 (1997), 68–90.

[25]George Downs and David Rocke Downs,*Tacit Bargaining: Arms Races, Arms Control* (Ann Arbor: University of Michigan Press 1990), 3.

[26]Robert Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca: Cornell University Press 1996).

degradation a costlier signal and thus more likely to achieve effects, but the results are complicated when examined carefully.[27] The Stuxnet operation launched against Iran, similar unsuccessful "left-of-launch" actions directed toward North Korea to prevent them from advancing its missile program, or even actions against Russia in response to the election hacks of 2016 are all examples of cyber degradation.

Cyber strategy therefore can be thought of as a modern variant of coercive diplomacy,

> a political-diplomatic strategy that aims to influence a [rival's] will or incentive structure. It is a strategy that combines threats of force, and if necessary, the limited and selective use of force in discrete and controlled increments, in a bargaining strategy … the aim is to induce an adversary to comply with one's demands, or to negotiate the most favorable compromise possible, while simultaneously managing the crisis to prevent unwanted military escalation.[28]

Unlike traditional perspectives on coercion, coercive diplomacy can involve positive inducements and is not singular focused on producing concessions (i.e., compellence) or stopping an action before it occurs (i.e., deterrence). Cyber strategies, like coercive diplomacy, are much broader than traditional perspectives on coercion. While rival states can and, as we show, do use cyber operations to compel, they more often than not use the digital domain to signal, steal, and engage in covert propaganda as a means of shaping long-term competition. These shaping operations form the foundation of Russian cyber strategy.

Cyber espionage: access, manipulation, and control

The Russian approach to cyber espionage involves not just stealing critical information but also leveraging it for propaganda value and signaling resolve as a means of changing the trajectory of future crises. By itself, cyber espionage does not achieve concessions. Rather, it is an additive means of accessing networks for future coercion and stealing sensitive information. Used in conjunction with broader propaganda campaigns, espionage can gain access to influence public opinion. These shaping actions do not achieve independent concessions but set the conditions for future crisis bargaining.

Espionage often runs parallel to broader manipulation efforts or set the conditions to follow on actions. One of Russia's cyber espionage toolkits, known as Snake/Uroburo/Tula, first appeared in 2005, targeting systems in the US,

[27] On how covert action can signal resolve through sinking costs, see Austin Carson and Keren Yarhi-Milo, 'Covert Communication: The Intelligibility and Credibility of Signaling in Secret', *Security Studies* 26/1 (2017), 124–156.

[28] Jack Levy, 'Deterrence and Coercive Diplomacy: The Contributions of Alexander George', *Political Psychology* 29/4, 539.

United Kingdom, and other Western European countries.[29] Beginning in mid-2013, Operation Armageddon, a cyber espionage campaign that relied predominantly on spearfishing, targeted Ukrainian security services. Spearfishing involves targeted e-mails and communications designed to lure a person into making their machine vulnerable to exploitation. The timing of the attack coincided with the final negotiations between Ukraine and the European Union Association Agreement.[30] Another Russia-linked cyber espionage campaign from a group known as Sandworm surfaced in 2009 based on zero-day exploits affecting Windows operating systems.[31] A zero-day exploit takes advantage of security vulnerabilities inherent in core software or hardware that has yet to be patched. In October 2014, Sandworm used BlackEngery 3 for multiple intrusions in Ukraine focusing on power companies and media outlets.[32] In 2016, Ukrainian power companies along with the finance and defense ministry reported temporary disruptions linked by iSight Partners and attributed them to Sandworm.[33] Espionage efforts such as these reflect how cyber espionage has dual use as a signaling mechanism. The intrusion both accesses critical information that may aid in future cyber coercive incidents as a crisis escalates and signals, ambiguously enough to limit retaliation, to promote Russian interests in external actors.

Cyber espionage is also a means of manipulation and undermining the institutions of opponents. A Russian group known as APT28, or Fancy Bear, similarly used malware to target groups of interest to the Russian state, including security ministries and journalists across the Caucasus region, the Polish and Hungarian governments, NATO, and the Organization for Security and Cooperation in Europe.[34] Unlike traditional Russia cyber-criminal groups, "APT 28 does not exfiltrate financial information from targets and it does not sell the information that it gathers for profit."[35] First discovered in 2011, Energetic Bear is a team that uses a common malware suite to infiltrated networks in the commercial space with economic or defense interests. Initially, the malware appeared on the networks of firms associated with the aviation industry and major defense contractors in the US and Canada. In 2013, the malware appeared on major energy firms such as Exxon-Mobil and British Petroleum.[36] Of note, Energetic Bear is "uniquely

[29]BAE Systems, *The Snake Campaign* (Feb. 2014); David Sanger and Steven Erlanger, 'Suspicion Falls on Russia as Snake Cyberattacks Target Ukraine's Government', *The New York Times,* 9 Mar. 2014.
[30]Brian Prince, '"Operation Armageddon" Cyber Espionage Campaign Aimed at Ukraine', *Security Week,* 28 Apr. 2015.
[31]Kim Zetter, 'Russian Sandworm Hack Has Been Spying on Foreign Governments for Years', *Wired,* (14 Oct. 2012.
[32]John Hultquist, *Sandworm team and the Ukrainian Power Authority Attacks* (FireEye 7 Jan. 2016).
[33]Pavel Polityuk, *Ukraine Investigates Suspected Cyber-attack on Kiev Power Grid* (Reuters 20 Dec. 2016).
[34]Threat Intelligence, *APT28: A Window into Russia's Cyber Espionage Operations* (FireEye 27 Oct. 2014).
[35]James Scott and Drew Spaniel, *Know Your Enemies 2.0* (Institute for Critical Infrastructure Technology 2016).
[36]MSS Global Threat Response, *Emerging Threat: Dragonfly/Energetic Bear – APT Group* (Symantec 30 Jun. 2014).

positioned to assist in a combination of digital and physical warfare for military or political purposes."[37] According to F-Secure, since 2008, MiniDuke, along with the CosmicDuke APT group, has acted as state-sponsored espionage organizations.[38] The Duke series first appeared after an 5 April 2008 speech by US President Obama advocating for a missile defense shield in Poland. In 2013, the group was linked to a spear phishing campaign targeting the Ukrainian ministry of foreign affairs.[39]

The style and content of Russian enabled cyber collectives reflect two logics of cyber espionage and its coercive potential. First, accessing target networks sets the conditions for follow-up operations. In military parlance, you prepare the environment for future action. Not only do you access critical networks and steal information altering the balance of information in a crisis, but even if the intrusion is revealed, the target is left wondering what else was stolen and what other networks are compromised.

Second, they demonstrate the utility of cyber espionage as a low-cost means of manipulating public opinion. In this respect, the actions are classic political warfare. Cyber is both a tool to manage crises indirectly and subvert public opinion and political will. In December 2014, "a well-known military correspondent for a large US newspaper was hit via his personal email address in December 2014, probably leaking his credentials. Later that month, Operation Pawn Storm attacked around 55 employees of the same newspaper on their corporate accounts."[40] Linked to APT 28, Pawn Storm infiltrated and disrupted TV5 Monde in France. In October 2015, Pawn Storm set up a fake VPN and fake Outlook Web Access server to conduct spear phishing attacks against the Dutch Safety Board investigating the Malaysian Airlines Flight 17 commercial airline flight that was shot down by a Russian Buk surface-to-air missile over Ukraine.

The manipulation of the 2016 US election

The 2016 US election hack demonstrates how Russia leverages cyber espionage as part of broader active measures campaign.[41] These campaigns do not lay the groundwork for future strikes as much as they focus on altering the perceptions of targeted domestic populations. As such, this event deserves extensive coverage as crucial case of Russian cyber activities. The

[37]Scott and Spaniel, *Know Your Enemies 2.0*, 29.
[38]Sarah Peters, 'MiniDuke, CosmicDuke APT Group Likely Sponsored by Russia', in *Dark Reading* (17 Aug. 2015).
[39]Sean Gallagher, 'Seven Years of Malware Linked to Russian State-Backed Cyber Espionage', *Arstechnica*, 17 Sept. 2015.
[40]Feike Hacquebord, *Operation Pawn Storm Ramps Up its Activities, Targets NATO, White House*, (Trend Micro 16 Aug. 2015).
[41]Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert, *Tainted Leaks: Disinformation and Phishing With a Russian Nexus* (Citizen Labs May 2017.

goal of the 2016 election hack was to achieve a broader psychological impact on American society while demonstrating to a Russian audience the corrupt nature of democratic institutions. The event serves as a demonstration of the utility of espionage as tool of manipulation. Often termed reflexive control or active measures, this form of espionage tries to influence the adversary through information control and manipulation aided by propaganda, operations all conducted short of war.

The Russian political warfare operation that culminated in the election hack started in 2015, before Donald Trump entered the presidential race. During the summer of 2015, Russia started the process by sending out thousands of phishing emails trying to get their targets to click on malicious links. Thomas Rid during Senate Testimony noted that about 2.4 percent of the attacks were successful in producing information.[42]

The breaches by Russia were not discovered until June 2016 with the *New York Times* noting that two different groups of Russian hackers (Cozy and Fancy Bear) penetrated the Democratic National Committee's (DNC) computer systems.[43] The goal was to monitor the DNC's communications while also exfiltrating their files including opposition research on Donald Trump. This information, in the tradition of KGB, could be used to either augment larger influence operations or as future blackmail material to gain leverage.

Perhaps the most devastating information grabs were the emails taken from Hillary Clinton's staff, further exacerbating a long-standing issue surrounding the question of stored emails on her personal home server. Campaign Chairman John Podesta's emails were stolen due to a typo on advice from an IT consultant to not answer a phishing email (illegitimate was corrected to legitimate).

The Dukes, or Cozy Bear as the Information Security (InfoSec) community calls them, group has been caught before operating in unclassified White House systems, the State Department, and various other US organizations. By the summer of 2015, they started to penetrate both DNC and Republican National Committee files.[44]

In March 2016, Fancy Bear or APT28 piled on. This intrusion thus demonstrates the uncoordinated nature of Russian cyber operations with duplicate processes occurring. Both actors were attacking the same targets, seemingly under the same mandate without overall coordination under similar instructions. Podesta's emails where released the same day as damning audio tape

[42]Thomas Rid, 'Disinformation: A Primer in Russian Active Measures and Influence Campaigns', Hearings before the Select Committee on Intelligence, United States Senate, One Hundred Fifteenth Congress, 30 Mar. 2017.
[43]David Sanger, 'D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump', *New York Times*, 14 Jun. 2016.
[44]Adam Greenberg, 'Russia Hacked "Older" Republican Emails, FBI Director Says', *Wired*, 10 Jan. 2017.

of Trump remaking on his ability to grab women hit the news cycle (the Billy Bush Bus tape incident).

Coordinated drops of information went on until late in the election cycle, demonstrating a high amount of collaboration between the brokers of information and the Trump campaign. Russian activities seemed to continue until a meeting between Obama and Putin at the G20 on 5 September where Obama warned against further attempts to influence the election. The information dumps stopped but Russian hackers continued to probe state level election voting systems looking for weaknesses.

In July 2016, Clinton's campaign suggested that Russia might be trying to sway the election.[45] Yet, it was not until 7 October that the Obama Administration formally accused Russia of interfering with the election.[46] A bipartisan statement was drafted but the Senate Republicans would not sign on the general statement supporting the noninterference in elections, suggesting it would tip the scales for the Democrats in the election.[47]

The issue was more complicated than simple Russian inference though; the main candidate encouraged the intrusions and information dumps. That Trump was "embracing an unlikely ally" in Wikileaks was certainly a troubling development.[48] Julian Assange, the leader of the organization, blames Hilary Clinton for his predicament and has openly sided with the Russian government, refusing to publish email troves of Russian documents. *Think Progress* counts 164 mentions of Wikileaks by Trump during campaign events.[49]

The coordination through information dumps, botnets supporting the releases, and the mentions by Trump himself demonstrate the power and collaboration needed to make political warfare insidious. As Clint Watts noted in Senate testimony, "part of the reason active measures have worked in the US election is because the Commander-in-Chief has used Russian active measures at times against his opponents."[50] Watts went on to note the many times fake information was released, passed, and amplified by bot networks and then parroted by the Trump campaign itself.

In September 2017, Facebook announced that the company had sold at least $150,000 in ads to Russian operatives after being called into private

[45]Eric Lichtblau, 'Computer Systems Used by Clinton Campaign Are Said to Be Hacked, Apparently by Russia', *New York Times*, 20 Jul. 2016.
[46]David Sanger and Charles Savage, 'U.S. Says Russia Directed Hacks to Influence Elections', *New York Times*, 7 Oct. 2016.
[47]Kaveh Waddell, 'Why Didn't Obama Reveal Intel About Russia's Influence on the Election?', *The Atlantic*, 11 Dec. 2016.
[48]Patrick Healy, David Sanger, and Maggie Haberman, 'Donald Trump Finds Improbable Ally in WikiLeaks', *New York Times*, 12 Oct. 2016.
[49]Judd Legum, 'Trump Mentioned WikiLeaks 164 Times in the Last Month of Election, Now Claims it Didn't Impact one Voter', *Think Progress*, 8 Jan. 2017.
[50]Aaron Rupar, 'Former FBI agent Details How Trump and Russia Team Up to Weaponize Fake News', *Think Progress*, 30 Mar. 2017.

questioning by the House of Representatives. "The Agency," a well-known Russian Troll farm, was linked to the ad buys. These ads seemed to seek to influence divisive internal conflict but amplifying issues such as Black Lives Matter. The ads ran from June 2015 to May 2017. As it stands, the *Daily Beast* estimates that, at a minimum, 23 million people saw the ads with a high-end estimate of 70 million.[51] The figure is based on an average of $6 in ad buys results in 1000 views with estimates increasing through targeting and voluntary sharing of the information.

Speculation that Russia was behind the attacks and information releases has been consistent since the issue was first reported in June 2016. A plethora of sources have indicated that the operation was sophisticated and bore the hallmarks of a Russian influence operation, starting with Cloudstrike, a prominent cyber security firm that the DNC turned to. News organizations including the *New York Times*, *Washington Post*, and later, *Politico* all released investigative reports on the operation. Thomas Rid noted in *Esquire* that researchers connected the command server for the malware targeting the DNC to a prior attack on German Parliament in 2015.[52]

In January 2017, the US Intelligence Community as a collective offered their assessment that Russian operations sought to "undermine public faith in the US democratic process, denigrate Secretary [Hillary] Clinton, and harm her electability and potential presidency."[53] The report identified the motive as Putin blaming Clinton personally for the release of the Panama Papers (a series of information dumps locating illicit banking methods) and protests in Russia in 2011 and 2012.

Cyber coercion is difficult, costly, and time-consuming. The Russian operation against the election started well before 2016 and continued past the actual vote. While there is no clear impact that can be detailed, the operation likely reinforced negative opinions of Hillary Clinton already held by Republican voters and supporters of Bernie Sanders. There is no evidence that the operation changed minds, no poll has ever been released that showed support for Trump was generated through Wikileaks. The question is if the hacks motivated individuals to reject Clinton and turn out to vote for Trump.

It appears likely that dozens of strategic mistakes lead to Clinton's loss, including not giving sufficient attention to the Rust belt, the inability to counter fears over immigration, James Comey note that Clinton's emails were under review again, and persistent gender bias. Yet, not having an

[51]Ben Collins, Kevin Poulsen, and Spencer Ackerman, 'Russia' Facebook Fake News Could Have Reached 70 Million Americans', *Daily Beast*, 8 Aug. 2017.
[52]Thomas Rid, 'How Russia Pulled Off the Biggest Election Hack in U.S. History', *Esquire*, 20 Oct. 2016.
[53]Director of National Intelligence, *Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytical and Cyber Incident Attribution* (6 Jan. 2017).

effective counter to Russian information warfare and its convenient network of allies was a costly mistake.

From the strategic perspective, the benefit to Russia was in causing chaos in its target. This classic tactic of Russian disinformation campaigns continues to yield unforeseen benefits for Russia. These manipulation strategies engage on all fronts, seeking to achieve effects in situations where Russia has few advantages. Changing the direction of the US government, or weakening the new President before they even take office, is an enormous benefit to Russia in that it confuses policy toward Ukraine, delays any action against Syria for human rights violations, and allows Russia's operations to continue in a similar fashion against Germany and France during their 2017 elections.

Yet, overall, the greatest benefit was likely a bit more subtle; American alliances are fractured and confused. The US paradoxically offers military hardware to its allies while also threatening trade wars with these very same countries. If confusion was the goal, Russia succeeded to dramatic effect. Cyber espionage can have a clear and coercive effect, but it is rare, contingent on many factors, and depends on the lack of trust in the target on critical sources of information to achieve results. By preparing for massive global catastrophes that might be a cyber 9/11 scenario, observers miss the more persuasive and insidious impact of Russia's complex attack and dissemination strategies.

Ukraine: a case study of combined effects

The ongoing conflict in Ukraine offers a portrait of how Russia combines cyber coercion with other instruments of conventional power. This is also a critical case in that it goes beyond the US election hack with the use of information operations in support of conventional military operations. Specifically, cyber campaigns in Ukraine seek to disrupt and delegitimize the country as a means of isolating Kiev and demonstrating the futility of the Ukrainian state.

Russia seeks more than manipulation; it seeks domination. According to Giles, "unlike Georgia … Russia already enjoyed domination of Ukrainian cyberspace, including telecommunication companies, infrastructure, and overlapping networks."[54] This access allowed them to wage a more sophisticated coercive campaign. That said, there is no evidence to suggest the Russian campaign is that sophisticated. Rather, the digital domain played a supporting role to Russian proxy military operations and propaganda efforts. Outside of Russia's fait accompli seizure of Crimea, these operations have produced no concessions beyond producing a frozen conflict. In this

[54]Kier Giles, 'Putin's Troll Factories', *Chatham House* 71/4 (2015).

respect, cyber-combined coercion in Ukraine demonstrated that cyber options are restrained even in war. The disruptive campaign was a testing ground for new operations and no operation to date has proved decisive enough for the Ukrainians to back down to Russian aggression.[55]

In late 2013, activists set up a protest camp in Kiev's independence square (Maidan), calling for deeper European integration and an end to rampant corruption. The events escalated after over 100 protesters were killed in 48 hours by a special police unit, the Berkut, causing the protests to escalate and pro-Russian President Viktor Yanukovych to flee. By 27 February 2014, reports of Russian operatives and "local militias" in Crimea started to appear paving the way for a March referendum for Crimea to join Russia. In early May, two regions dominated by ethnic Russians, Donetsk and Luhansk, held referendums, declaring independence.

Paralleling the escalating crisis in late 2013, Ukrainian officials noted that "network vandalism had given way to a surge in cyber espionage, from which commercial cyber security companies developed a list of colorful names: RedOctober, MiniDuke, NetTraveler, and many more."[56] Koval claims that Russia conducted constant, low-level disruption campaigns against Ukraine using "botnet-driven" DDoS often "in retaliation for unpopular government initiatives."[57] Botnet-driven DDoS attacks involve overloading servers with content generated by hacked computers, usually without the knowledge of the user. Glib Pakharenko offers an insider's account of the cyberattacks during the Maidan protests:

> the cyber attacks began on 2 December 2013 when it was clear that protesters were not going to leave Maidan. Opposition websites were targeted by DDoS attacks, the majority of which came from commercial botnets employing BlackEngery and Dirt Jumper malware…. As Ukrainian opposition groups responded with their DDoS attacks, cyber-criminal organizations proactively reduced their use of the Ukrainian Internet Protocol (IP) space rerouting their malware communications through Internet Service Providers (ISP) in Belarus and Cyprus, which meant that, for the first item in years, Ukraine was not listed among the leading national purveyors of cybercrime.[58]

In early 2014, Ukrainian civilian and government networks were subject to a barrage of DDoS attacks. Cyber Berkut, a pro-Russian hacktivist group, a major proxy group with links to the Russian government, organized in the incidents. The threat actor took their name from the former special police unit disbanded in the wake of the Maidan protests, producing an illusion that pro-Moscow Ukrainians were rebelling against Kiev. CrowdStrike has

[55]Andy Greenberg, 'How an Entire Nation Became Russia's Test Lab for Cyberwar', *Wired*, 20 Jun. 2017.
[56]Nikolay Koval, 'Revolution Hacking', in Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO Cooperative Cyber Defence Center of Excellence 2015).
[57]Koval 'Revolutionary Hacking', 55.
[58]Koval 'Revolutionary Hacking', 50.

linked the group to the Russian government based on forensic data and parallels between messages put out by CyberBerkut and "messaging delivered by Russia-owned state media."[59] According to reporting by the firm,

> there are significant parallels between the current techniques employed by CyberBerkut and those used in previous conflicts associated with Russia, namely the conflict in Estonia in 2007. These techniques, leveraging Soviet-style deception, propaganda, and denial tactics, suggest a process in which the first iterations of online warfare implemented in Estonia are now being perfected in Ukraine.[60]

Cyber Berkut's actions ranged from disrupting mobile phone networks as a means of complicating Ukraine's response to the ongoing crisis to more complex, foreign disruptions designed to isolate and delegitimize Kiev.[61] In March 2014, Cyber Berkut claimed credit for a DDoS targeting three NATO websites. In October of that same year, the group was linked to a DDoS attack against German Ministry of Defense. In January 2015, a DDoS attack against the German Parliament and Chancellor Angela Merkel's websites was attributed to the group.

Over the course of 2014, Cyber Berkut also conducted prominent website defacements, placing narratives and symbols that matched Russian propaganda linking the Ukrainian conflict to fascism. In August 2014, the group hacked Polish websites, including the stock exchange, and defaced them with images of the Holocaust.[62] In November 2014, during Vice President Joe Biden's visit to Kiev, the group defaced several Ukrainian government websites with messages stating, "Joseph Biden is the fascists" master.'[63] In December 2014, the group hacked multiple electronic billboards in Kiev and replaced advertisements with video's showing graphic images of civilian casualties and portraying Ukrainian officials and anti-Russian activists as war criminals.

The most significant disruptive effort involved combining cyber espionage and disruption alongside propaganda to undermine the legitimacy of the Ukrainian election in 2014. According to Ian Gray, an analyst at Flashpoint, Russia seeks to achieve a low-cost disruption "by organizing a disinformation campaign attacking confidence in the election itself."[64] In May 2014, CyberBerkut "infiltrated Ukraine's central election computers and deleted key files, rendering the vote-tallying system inoperable. The next day, the hackers declared they had 'destroyed the computer network

[59]CrowdStrike, *2015 Global Threat Report* (2015).
[60]CrowdStrike, *2015 Global Threat Report*.
[61]Sam Masters, 'Ukraine Crisis: Telephone Networks are First Casualty of Conflict', *The Independent*, 25 Mar. 2014.
[62]Cory Bennett, 'Hackers breach the Warsaw Stock Exchange', *The Hill*, Oct. 2014.
[63]Vitaly Shevchenko, 'Ukraine Conflict: Hackers Take Sides in Virtual War', *BBC*, 20 Dec. 2014.
[64]Shaun Waterman, 'Russia Seeks to Discredit, Not Hack Election Results', *Cyberscoop*, 7 Nov. 2016.

infrastructure' for the election, spilling e-mails and other documents onto the web as proof."[65] Compounding the intrusion, the group installed malware that attempted to manipulate the results, showing a victory by ultranationalists, a key theme reinforced by broader Russian propaganda reflecting the Maidan as a Fascist revolution. According to Ukrainian cyber security experts, "preparation for such an attack does not happen overnight; based on our analysis of Internet Protocol (IP) activity, the attackers began their reconnaissance in mid-March 2014 – more than two months prior to the election."[66]

Another combined strategy on display in Ukraine was the use of false flag operations designed to not only hide attribution but also discredit the target, a tactic consistent with Soviet practices. False flags are a form of covert action designed to manipulate perception with deep historical roots. The term refers to making it seem as if an act was carried out under another nation's flag. A group attempts to conceal its involvement by creating the perception that a separate group carried out some act of sabotage, subversion, or physical attack. Under the handle Anonymous Ukraine, in March 2014, Russia released fabricated documents claiming to show evidence that the US Army Attaché was coordinating a series of false flag attacks designed to look like Russian Special Forces with the Ukrainian Army. In March 2015, CyberBerkut released documents said to be hacked from US defense contractors and Ukrainian government showing US plans to move weapons into Ukraine. Later that month, the group also released documents said to be hacked from the Ukrainian military showing that the government in Ukraine supplied weapons to the Islamic State. The group also released documents said to be hacked from the Soros Foundation showing that George Soros was pressuring American officials to provide lethal assistance to Ukraine.

In all cases, these false flag operations were picked up and broadcast through Russian media outlets and operatives on social media sites. Russia uses troll factories to shape how its public digests western media and distort unfavorable stories for foreign audiences.[67] For example, in March 2015, false flag operation citing evidence that the Ukrainian state-owned defense conglomerate Ukroboronprom collaborated with the Qatari government to supply surface-to-air missiles was reported on outlets such as *Sputnik International*, a state-controlled Russian media outlet.

This disinformation and delegitimizing campaign built on earlier network exploitation and cyber espionage. Access to Ukrainian information networks allowed them to spearfish Ukrainian officials. Hackers use typosquatting, registering a domain with just a misplaced letter, to spear phish

[65]Mark Clayton, 'Ukraine election narrowly avoided "wanton destruction" from hackers', *Christian Science Monitor* (17 Jun. 2014).
[66]Koval, 'Revolutionary Hacking', 60.
[67]Giles, 'Putin's Troll Factories'.

users accessing the website of Ukrainian President Petro Poroshenko.[68] Similar social engineering hacks were used as part the US presidential election hack, where the two groups, CozyBear and Fancy Bear, spearfished Democratic operatives at the DNC.[69] The same groups were also linked to spearfishing attacks on DC-area think tanks after the US presidential election.

As the Ukrainian crisis continued, Russia found new ways of combining cyber effects with irregular and conventional military operations. First, Russia employed traditional military operations to isolate information objectives. For example, in November 2014, Russian operatives sabotaged cables connecting the Crimean Peninsula to Ukraine.[70] Conventional operations helped isolate a target. Russia achieved similar effects in cyberspace. According to Glib Pakharenko:

> Russian signals intelligence (SIGINT) including cyber espionage, has allowed for very effective combat operations planning against the Ukrainian Army. Artillery fire can be adjusted based on location data gleaned from mobile phones and Wi-Fi networks. GPS signals can also be used to jam aerial drones. Ukrainian mobile traffic can be rerouted through Russian GSM infrastructure via a GSM signaling level (SS7) attack; in one case this was accomplished through malicious VLR/HLR updates that were not properly filtered. Russian Security Services also use the internet to recruit mercenaries.[71]

Second, Russia employed cyber methods to degrade Ukrainian military capabilities. In 2016, the cyber security firm Crowdstrike reported that Russia used an Android-based malware to infect apps Ukrainian units were using to compute the math required for targeting artillery. These infections enabled digital reconnaissance and helped Russian units geolocate Ukrainian artillery formations and preemptively strike them.[72] While there is some debate as to the effectiveness of this operation, with Crowdstrike altering the estimates from 80 percent effectiveness in targeting Ukraine to 15–20 percent, that Ukrainian artillery was using basic apps for targeting demonstrates the potential vulnerabilities that cyber operations can exploit in support of conventional military operations.

Third, Russia employed earlier cyber espionage campaigns to activate malware capable of degrading Ukrainian critical infrastructure. In October 2014, Sandworm used BlackEngery 3 to gain access to power plants and then insert KillDisk malware, a program similar to destructive systems used

[68]Patrick Tucker, 'The Same Culprits That Targeted US Election Boards Might Have Also Targeted Ukraine', *Defense One*, 3 Sep. 2016.
[69]Jeff Stone, 'Meet Fancy Bear and Cozy Bear, Russian Groups Blamed for DNC Hack', *Christian Science Monitor*, 15 Jun. 2016.
[70]Chris Baraniuk, 'Could Russian Submarines Cut off the Internet?', *BBC*, 26 Oct. 2015.
[71]Pakharenko, 55.
[72]Adam Myers, *Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units* (CrowdStrike 22 Dec. 2016).

during the 2014 Ukrainian election.[73] Soon after the intrusion, some Ukrainian power plants went offline, though analysts still cannot draw a direct connection to KillDisk. Blackenergy 2015 and new CrashOverride 2016 are other critical infrastructure-targeting strands of malware that have been found in Ukrainian power plants.

Fourth, Russia integrated their operations with cyber disruption efforts paralleling broader disinformation campaigns. Russia weaponized social media to promote its narrative. Russian groups built redirects to steer users away from websites to Russian propaganda. For example, in 2015,

> cybercriminals helping spread pro-Russia messaging by artificially inflating video views and ratings on a popular video website. The campaign began with the infamous Angler exploit kit infecting victims with the Bedep trojan. Infected machines were then forced to browse sites to generate ad revenue, as well as, fraudulent traffic to a number of pro-Russia videos.[74]

Analysts linked the same malware to Russian cybercrime groups who used it to steal $45 million dollars from banks.[75]

In effect, Russia practices a new style of information operations designed "not to rebut but to obfuscate."[76] These operations rely

> on the fact that Western governments simply lack resources that would be required systematically to refute or debunk the huge number of stories put out, and on the Western media's professional obligation to report both sides of the story, thereby giving a veneer of legitimacy to Russian fabrications.[77]

Although Russian information and cyber operations reflect a degree of innovation not yet seen to such an extent in international campaigns, it is unclear if these strategies exhibit any novel utility. The media often seems to either ignore the implications of efficacy of cyber operations or present the issue from a purely partisan perspective (i.e., Russia did it but Trump's election is legitimate). These questions are too important to be investigated from a superficial perspective. The efficacy of cyber operations is critical and few have examined the issue empirically. Our case study here and the work of Kostyak and Zhukov demonstrate limited coercive utility through cyber espionage means.[78]

[73]Hultquist, *Sandworm team*.
[74]Rami Kogan, *Bedep Trojan Malware Spread by the Angler Exploit Kit gets Political* (Trustwave 29 Apr. 2015).
[75]Nick Biasini, 'Connecting the Dots Reveals Crimeware Shake-Up', *Talso*, 7 Jul. 2016.
[76]Nigel Inkster, 'Information Warfare and the US Presidential Election', *Survival* 58/5 (2016), 23–32.
[77]Inkster, 'Information Warfare'.
[78]Nadia Kostyak and Yuri Zhukov, 'Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?', *Journal of Conflict Resolution* (Forthcoming).

Conclusion

Russia prefers cyber disruptions that harass and sow discontent, which fail to coerce in a direct manner. The Russian approach to cyber strategy appears to be more about ambiguous signaling and amplifying propaganda than it does direct compellence. Russian cyber activities continue the Soviet approach to active measures, political warfare optimized to manipulate target populations and disrupt rivals from within. Due to these strategies, degradation efforts do not generate concessions in a manner similar to the cyber superpower, the US.

The Russian case offers insights into how states combine cyber operations with the military instruments of power or conventional information operations. Moscow tends to use cyberattacks in three waves: prior to the conflict to delegitimize and distract their rival, during the conflict to support combat operations, and after the initial fighting to create chaos that, consistent with active measures, undermines the legitimacy of the target state. However, Russian use of cyber operations during conflict does not appear to alter the outcomes or make concessions more likely. Of note, both the conflicts in Georgia and Ukraine have resulted in frozen conflicts, not decisive victories.

When Russia employs cyber coercion against Western rivals outside of its former Soviet space, these states tend to counter with diplomatic and economic instruments. These counters are consistent with a "tit-for-tat" logic, limited horizontal escalation designed to check Moscow and limit a dangerous conflict spiral. When cyber coercion is used against targets in the Baltics, the states counter by strengthening their ties to NATO and enhancing their domestic military.

Finally, Russian cyber strategy, in addition to reflecting tenets of Soviet-era active measures, focuses on soft targets, including civilian networks. These methods have largely been unsuccessful beyond the debatable example of the US Election hack in 2016. As opposed to the US, Russia tends to amplify propaganda with bots and troll farms rather than more traditional diplomatic coercion. To date, these operations have yet to produce concessions. In the end, Moscow acts more like a rogue state undermining the norm against targeting critical infrastructure than it does like a responsible actor in the digital domain.

Russia still has not unleashed the full potential of cyber operations against critical energy targets. They have not resorted to direct cyber violence, destroying infrastructure that results in immediate death such as blowing up a power plant, digitally sabotaging vital public infrastructure like sewers or water treatment, or hacking personal medical devices. Rather, Moscow's network intrusions on the battlefield in Ukraine indirectly helped military units increase their lethality.

Russia's aggressive, albeit unsuccessful, cyber operations threaten stability in cyberspace by targeting critical systems and illustrate how political warfare works in the digital domain. This case demonstrates the limits and logic of cyber strategies. While cyber operations do not produce significant effects on their own, they support other lines of effort including manipulating perception and sowing chaos in targeted populations.

Rather than herald a revolutionary break in the history of warfare, the employment of cyber operations between rivals can create strategic stability and reinforce traditional power dynamics. For Gartzke and Lindsay, there is a distinct stability–instability paradox in cyberspace.[79] The open architecture of the internet creates a unique vulnerability. If the target of coercion disconnects, they are no longer as vulnerable. Therefore, the aggressor has to operate either covertly or beneath a threshold to avoid retaliation. Furthermore, the aggressor knows that if it crosses that threshold, they risk a cross-domain response. A state could respond with economic sanctions, as seen in the Russia hack of US elections, or outright military force.

Since most forms of cyber strategy investigated here are optimized for covert action, they reflect a desire to signal resolve while keeping conflicts limited. Like covert action, cyber works in the shadows and can help rivals engage in tacit cooperation "to steer dangerous encounters to the backstage as a way to safeguard the external impression of their encounter as a limited conflict."[80] Plausible deniability in cases where attribution is fairly obvious (e.g., Russian incursions into Ukraine in 2014–15 or attacking the US election in 2016) works not necessarily to hide the identity of the attacker but rather to provide justification for the defender to moderate their response.

This signaling dynamic leaves us with the question of how do you compel a rival state if they do not know they have been breached in the first place? That is, how can covert action compel rivals? In 2016, the Obama Administration planted "cyber bombs" in Russian networks as a retaliation for the election hack.[81] Yet, if you do not signal the opposition that you have this deadly tripwire installed, how can you expect to affect their behavior and compel them to back down in their efforts to attack the American democratic process? Furthermore, if you send too explicit a signal, you give the target the opportunity to patch their network reducing your coercive leverage.

Despite the promise of quick wins in the digital domain, there are complex signaling dynamics in cyberspace that make producing concessions difficult. The future of cyber operations could reflect a drastically increased utility for

[79]Gartzke and Lindsay, 'Coercion through the Cyberspace'.
[80]Austin Carson, 'Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War', *International Organization* 70/1 (2016), 105.
[81]Austin Carson, 'Obama Used Covert Retaliation in Response to Russian election Meddling. Here's Why', *Washington Post*, 29 Jun. 2017.

the efficacy of cyber operations. If planning is based on the current effectiveness of Russian operations, the best advice notes that their operations are restrained, generally fail to achieve results, and seek to limit escalation. Understanding this process of cyber strategies is a key task and results demonstrate more bluff and bluster than bending the will of the enemy.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Benjamin Jensen, Ph.D., holds a dual appointment as an associate professor at Marine Corps University and as a scholar-in-residence at American University, School of International Service. He is also a senior nonresident fellow at the Atlantic Council.

Brandon Valeriano, Ph.D., is the Donald Bren Chair of Armed Politics at Marine Corps University.

Ryan Maness, Ph.D., is an assistant professor at the Naval Postgraduate School.

Bibliography

BAE Systems, *The Snake Campaign* (Feb. 2014).

Baraniuk, Chris, 'Could Russian Submarines Cut off the Internet?', *BBC*, 26 Oct. 2015.

Beaufre, Andre, *An Introduction of Strategy* (London: Faber and Faber 1965 R.H. Barry translation).

Bennett, Cory, 'Hackers Breach the Warsaw Stock Exchange', *The Hill*, Oct. 2014.

Biasini, Nick, 'Connecting the Dots Reveals Crimeware Shake-Up', *Talso*, 7 Jul. 2016.

Borghard, Erica and Shawn Lonergan, 'The Logic of Coercion in Cyberspace', *Security Studies* 26/3 (2017), 452–81. doi:10.1080/09636412.2017.1306396

Carson, Austin, 'Facing off and Saving Face: Covert Intervention and Escalation Management in the Korean War', *International Organization* 70/1 (2016), 103–31. doi:10.1017/S0020818315000284

Carson, Austin, 'Obama Used Covert Retaliation in Response to Russian Election Meddling. Here's Why', *Washington Post*, 29 Jun. 2017.

Carson, Austin and Keren Yarhi-Milo, 'Covert Communication: The Intelligibility and Credibility of Signaling in Secret', *Security Studies* 26/1 (2017), 124–56. doi:10.1080/09636412.2017.1243921

Clayton, Mark, 'Ukraine Election Narrowly Avoided 'Wanton Destruction' from Hackers', *Christian Science Monitor* (17June2014).

Collins, Ben, Kevin Poulsen, and Spencer Ackerman, 'Russia' Facebook Fake News Could Have Reached 70 Million Americans', *Daily Beast*, 8 Aug. 2017.

CrowdStrike, *2015 Global Threat Report*, (2015).

Director of National Intelligence, *Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytical and Cyber Incident Attribution* (6 Jan. 2017).

Downs, George and David Rocke Downs, *Tacit Bargaining: Arms Races, Arms Control* (Ann Arbor: University of Michigan Press 1990).
Fearon, James D., 'Rationalist Expectations for War', *International Organization* 49/3 (1995), 379–414. doi:10.1017/S0020818300033324
Fearon, James D., 'Signaling Foreign Policy Interests Tying Hands versus Sinking Costs', *Journal of Conflict Resolution* 41/1 (1997), 68–90. doi:10.1177/0022002797041001004
Freedman, Lawrence, 'Strategic Studies and the Problem of Power', in Thomas Mahnken and Joseph A. Maiolo (eds.), *Strategic Studies: A Reader* (New York: Routledge 2008).
Gallagher, Sean, 'Seven Years of Malware Linked to Russian State-Backed Cyber Espionage', *Arstechnica*, 17 Sept. 2015.
Gartzke, Erik and Jon R. Lindsay, 'Coercion through the Cyberspace: The Stability-Instability Paradox Revisited', in Kelly Greenhill and Peter Krause (eds.), *The Power to Hurt in the Modern World* (Oxford: Oxford University Press 2017).
George F. Kennan on Organizing Political Warfare, 'History and Public Policy Program Digital Archive, Obtained and Contributed to CWIHP by A. Ross Johnson', *Cited in his book Radio Free Europe and Radio Liberty, Ch1 n4 – NARA release courtesy of Douglas Selvage. Redacted final draft of a memorandum dated May 4, 1948, and published with additional redactions as document 269, FRUS, Emergence of the Intelligence Establishment*, 30 Apr. 1948.
Gerasimov, 'The Value of Science in Prediction', in *Military-Industrial Kurier* (27Feb.2013).
Giles, Kier, 'Putin's Troll Factories', *Chatham House* 71/4 (2015).
Greenberg, Adam, 'Russia Hacked "Older" Republican Emails, FBI Director Says', *Wired*, 10 Jan. 2017.
Greenberg, Andy, 'How an Entire Nation Became Russia's Test Lab for Cyberwar', *Wired*, 20 Jun. 2017.
Hacquebord, Feike, *Operation Pawn Storm Ramps up Its Activities, Targets NATO, White House* (Trend Micro 16 Aug. 2015).
Healy, Patrick, David Sanger, and Maggie Haberman, 'Donald Trump Finds Improbable Ally in WikiLeaks', *New York Times*, 12 Oct. 2016.
Heuser, Beatrice, *The Evolution of Strategy: Thinking War from Antiquity to the Present* (New York: Cambridge University Press 2010).
Hulcoop, Adam, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert, *Tainted Leaks: Disinformation and Phishing with a Russian Nexus* (Citizen Labs May 2017).
Hultquist, John, *Sandworm Team and the Ukrainian Power Authority Attacks* (FireEye 7 Jan. 2016).
Inkster, Nigel, 'Information Warfare and the US Presidential Election', *Survival* 58/5 (2016), 23–32.
Isaac, Mike and Daisuke Wakabayashi, 'Russian Influence Reached 126 Million Through Facebook Alone', *New York Times*, 30 Oct. 2017.
Jensen, Benjamin, *Forging the Sword: Doctrinal Change in the U.S. Army* (Pal Alto: Stanford University Press 2016).
Kaspersky Labs, *Lazarus under the Hood* (25 Nov. 2017).
Kogan, Rami, *Bedep Trojan Malware Spread by the Angler Exploit Kit Gets Political* (Trustwave 29 Apr. 2015).
Kostyak, Nadia and Yuri Zhukov, 'Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?', *Journal of Conflict Resolution* (forthcoming).

Koval, Nikolay, 'Revolution Hacking', in Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO Cooperative Cyber Defence Center of Excellence 2015), 55–65.
Legum, Judd, 'Trump Mentioned WikiLeaks 164 Times in the Last Month of Election, Now Claims It Didn't Impact One Voter', *Think Progress*, 8 Jan. 2017.
Levy, Jack, 'Deterrence and Coercive Diplomacy: The Contributions of Alexander George', *Political Psychology* 29/4, 537–52.
Libicki, Martin, *Crisis and Escalation in Cyberspace* (Santa Monica: Rand Corporation 2012).
Lichtblau, Eric, 'Computer Systems Used by Clinton Campaign are Said to Be Hacked, Apparently by Russia', *New York Times*, 20 Jul. 2016.
Lindsay, Jon R., 'Stuxnet and the Limits of Cyber Warfare', *Security Studies* 22/3 (2013), 365–404. doi:10.1080/09636412.2013.816122
Lindsay, Jon R., 'The Impact of China on Cybersecurity: Fiction and Friction', *International Security* 39/3 (2014), 7–47.
Masters, Sam, 'Ukraine Crisis: Telephone Networks are First Casualty of Conflict', *The Independent*, 25 Mar. 2014.
MSS Global Threat Response, *Emerging Threat: Dragonfly/Energetic Bear – APT Group* (Symantec 30 Jun. 2014).
Myers, Adam, *Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units* (CrowdStrike 22 Dec. 2016).
Osgood, Robert, *The Entangling Alliance* (Chicago: University of Chicago Press 1962).
Pape, Robert, *Bombing to Win: Air Power and Coercion in War* (Ithaca: Cornell University Press 1996).
Peters, Sarah, 'MiniDuke, CosmicDuke APT Group Likely Sponsored by Russia', in *Dark Reading* (17 Aug. 2015).
Polityuk, Pavel, *Ukraine Investigates Suspected Cyber-Attack on Kiev Power Grid* (Reuters 20 Dec. 2016).
Prince, Brian, '"Operation Armageddon" Cyber Espionage Campaign Aimed at Ukraine', *Security Week*, 28 Apr. 2015.
Rid, Thomas, 'How Russia Pulled off the Biggest Election Hack in U.S. History', *Esquire*, 20 Oct. 2016.
Rid, Thomas, 'Disinformation: A Primer in Russian Active Measures and Influence Campaigns', Hearings before the Select Committee on Intelligence, United States Senate, One Hundred Fifteenth Congress, 30 Mar. 2017.
Rupar, Aaron, 'Former FBI Agent Details How Trump and Russia Team up to Weaponize Fake News', *Think Progress*, 30 Mar. 2017.
Sanger, David, 'D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump', *New York Times*, 14 Jun. 2016.
Sanger, David and Steven Erlanger, 'Suspicion Falls on Russia as Snake Cyberattacks Target Ukraine's Government', *The New York Times*, 9 Mar. 2014.
Sanger, David and Charles Savage, 'U.S. Says Russia Directed Hacks to Influence Elections', *New York Times*, 7 Oct. 2016.
Schelling, Thomas, *Strategy of Conflict* (Cambridge: Harvard University Press 1960).
Schelling, Thomas, *Arms and Influence* (New Haven: Yale University Press 1968).
Scott, James and Drew Spaniel, *Know Your Enemies 2.0* (Institute for Critical Infrastructure Technology 2016).
Sharp, Travis, 'Theorizing Cyber Coercion: The 2014 North Korea Operation against Sony', *Journal of Strategic Studies* (2017).

Shevchenko, Vitaly, 'Ukraine Conflict: Hackers Take Sides in Virtual War', *BBC*, 20 Dec. 2014.

Slayton, Rebecca, 'What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessments', *International Security* 41/3 (2016), 72–109.

Stone, Jeff, 'Meet Fancy Bear and Cozy Bear, Russian Groups Blamed for DNC Hack', *Christian Science Monitor*, 15 Jun. 2016.

Threat Intelligence, *APT28: A Window into Russia's Cyber Espionage Operations* (FireEye 27 Oct. 2014).

Tucker, Patrick, 'The Same Culprits That Targeted US Election Boards Might Have Also Targeted Ukraine', *Defense One*, 3 Sept. 2016.

Valeriano, Brandon, Ben Jensen, and Ryan Maness, *Cyber Strategy: The Changing Character of Cyber Power and Coercion* (New York: Oxford University Press 2018).

Waddell, Kaveh, 'Why Didn't Obama Reveal Intel about Russia's Influence on the Election?', *The Atlantic*, 11 Dec. 2016.

Waterman, Shaun, 'Russia Seeks to Discredit, Not Hack Election Results', *Cyberscoop*, 7 Nov. 2016.

Zetter, Kim, 'Russian Sandworm Hack Has Been Spying on Foreign Governments for Years', *Wired*, 14 Oct. 2012.