The Hybrid Threat to NATO Unity:

Recommendations for NATO and EUCOM

Word Count: 3008 words

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
23-02-2021	FINAL	N/A

4. TITLE AND SUBTITLE

The Hybrid Threat to NATO Unity: Recommendations for NATO and EUCOM

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

LCDR Mark D. Knorr, USN

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Writing & Teaching Excellence Center
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the curriculum. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Malign actors' recent success in subverting North Atlantic Treaty Organization (NATO) security and European Union (EU) prosperity elevated hybrid warfare to the forefront of deniable activities in great power competition. Russia is now conducting a grey zone campaign focused on exploiting information networks, degrading critical infrastructure, and influencing the populous. U.S. European Command (EUCOM) planners must respond to Russia's militarization of cyberspace by leading NATO efforts to mature a robust and legitimate cyber defense. Only a whole-of-alliance approach can mitigate the destabilizing impact of hybrid warfare enabled by cyber-attacks, political subversion, and domestic influence operations across the continent of Europe. Furthermore, the establishment of norms and standards for cyber conduct under international law can augment EUCOM's efforts and ensures legitimacy in the fight against a subversive grey zone threat. Similarly, NATO must develop a robust cyber surveillance and response capability across all member-states to reinforce international law and protect state sovereignty from cyber assault. Ultimately, NATO should round-out these advances by maintaining a cyber deterrent capability focused on policy and practice to effectively message capability and intent in order to safeguard the unity of the alliance and defend forward.

15. SUBJECT TERMS (Key words)
EUCOM, Cyber, NATO

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Director, Writing Center
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	N/A	15	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-6499

Standard Form 298 (Rev. 8-98)

The North Atlantic Treaty Organization (NATO) finds itself struggling to unite behind a comprehensive strategy to address threats below the level of armed conflict. The alliance remains under assault from state and non-state actors keen to exploit and degrade international cooperation; this challenge places the transatlantic partnership's longevity and effectiveness at risk. Malign actors' recent success in subverting NATO security and European Union (EU) prosperity elevated hybrid warfare to the forefront of deniable activities through their control of the cyber domain. Russia is now conducting a grey zone campaign focused on exploiting information networks, degrading critical infrastructure, and influencing the populous. Moscow's brazen actions demonstrate confidence that NATO's division will prevent a unified allied response. Russian tactics "undermine the liberal and constitutional order in Europe" and represent the finest of low-cost, high-yield approaches to hybrid warfare.[1] This combined approach is effective in the face of NATO and western Europe's immature cyber defense structures, network security, and control of the political narrative.

Therefore, NATO must take a whole-of-alliance approach to mitigate the destabilizing impact of hybrid warfare enabled by cyber-attacks, political subversion, and domestic influence operations in order to safeguard the unity of the alliance and defend forward across the continent of Europe. This paper will identify and detail three main lines of effort for NATO in response to the ongoing threat of hybrid warfare. First, NATO should use its power and example as the premier liberal democratic institution to establish norms and standards in the cyber domain under international law. Second, NATO should develop a cyber surveillance and response capability across all member-states to reinforce international law and protect state sovereignty from cyber

[1] Stephanie Pezard, Andrew Radin, Thomas S. Szayna, and F. Stephen Larrabee, *European Relations with Russia: Threat Perceptions, Responses, and Strategies in the Wake of the Ukrainian Crisis*, (Santa Monica, CA: RAND Corporation, 2017), 18, https://www.rand.org/pubs/research_reports/RR1579.html.

assault. Lastly, NATO should round-out these advances by maintaining a cyber deterrent capability focused on policy and practice to effectively message capability and intent. This paper closes with specific recommendations provided for the Commander, U.S. European Command (EUCOM), to reinforce and directly support the proposed lines of effort.

The Real Consequences of Cyberwarfare

Among other things, Russian cyberattacks threaten critical security infrastructure, shape public perception, and provide access to private information that give Moscow the upper hand in great power competition. The prevalence of cyber-attacks grew over the last fifteen years as Russian-state, and state-sponsored actors tested defenses and successfully impacted the industrial, economic, and intellectual security of NATO and European Union countries.[2] The NotPetya attack in Ukraine in 2017 stands as the most damaging widespread cyberattack in Eastern Europe to date.[3] This attack, attributed to Russia, demonstrates both the capability and resolve of Russian meddling and the susceptibility of linked digital information networks. The Cyberspace Solarium Commission reports that NotPetya "exploited operating system vulnerabilities in wide use across innumerable private- and public-sector applications" and "quickly spread from targeted Ukrainian banks, payment systems, and federal agencies to power plants, hospitals, and other life-critical systems worldwide."[4] The far-reaching effects of the malware-induced service interruption and follow-on instability cost industry leaders throughout Europe, such as Maersk and FedEx, nearly $10 billion in losses.[5] NotPetya placed NATO

[2] Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare*, CNA, March 2017, 27-29, https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.
[3] Cyberspace Solarium Commission, *Final Report*, March 2020, 8, https://www.solarium.gov/report.
[4] Cyberspace Solarium Commission, *Final Report*, 8.
[5] Cyberspace Solarium Commission, *Final Report*, 8.

critical infrastructure throughout Europe at risk and served as a wake-up call to the threat of a weaponized cyber domain.

The instability resultant from a cyberattack similar to NotPetya can shake a populous to its core and represents a violation of sovereignty not previously achievable outside of war. NotPetya struck Ukraine just one year after vital infrastructure fell victim to attacks on the power grid, resulting in blackouts throughout Kyiv on two separate occasions.[6] These types of attacks fall short of violence, but their effects are far more sinister and serve to reinforce an overarching political strategy. The attack's true measure of success was that it manifested an atmosphere of disorder and demonstrated a lack of control by the authorities while allowing perpetrators to access personal and corporate data.[7] Furthermore, the attacks sowed doubt in state control and the rule of law by undermining state sovereignty and the institutions of governance.

Russia's application of cyberwarfare serves their political ends by undermining the authority of the democratic rule of law throughout Europe; however, Moscow's strategic hacking tactics also provide them the benefit of unfettered access to privileged information. This access supports Russia's desire to "inform its decision-making and benefit its economic interests."[8] Russian-state espionage groups, most notably APT28 or Fancy Bear, routinely gain access to industrial, government, and military plans giving the Kremlin the upper hand in decision-making.[9] The theft of industrial practices provides Russian companies with a lifeline to maintain prosperity even in the face of sanctions, effectively undermining the international community's power to penalize Russia's malign acts. By mastering this form of hybrid warfare, Russia

---

[6] Laurens Cerulus, "How Ukraine became a test bed for cyberweaponry," *Politico*, 14 February 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.
[7] Cerulus, "How Ukraine."
[8] National Counterintelligence and Security Center, *Economic Espionage Counter Intel and Security,* 8, 12.
[9] National Counterintelligence and Security Center, *Economic Espionage*, 8, 12.

developed a proven method to advance their strategic objectives while increasing their industrial position and denying the liberal international order's use of nonviolent economic leverage.

Disrupting the Democratic Narrative Through Political Subversion

Russia seeks to fundamentally alter the direction of European politics through exploitation and subversion focused on discounting the democratic election process. European democracies are under surveillance and assault as Russian actors work to shape or discredit public policy through their strategic application of an aggressive hybrid warfare campaign. Europe feels this pressure from the ever-present turmoil in the Baltic States to the threat assessments among NATO leaders such as Germany and France.[10] Moscow orchestrates this campaign to degrade cooperation among alliance members by unraveling strategic cohesion and promoting national instability.

Russia's preferred view of Europe is one that enables their freedom of action and self-interest. Therefore, Russian agents employ targeted cyber-enabled misinformation campaigns to identify and discredit political and ideological threats to their interests. This challenge is no surprise to NATO member-states; however, they differ on the perceived threat and their vulnerability.[11] This mismatch within the alliance compounds the danger of Russian meddling as it prevents a unified response from the significant players of Europe. Furthermore, the vulnerabilities inherent to interconnected networks create continent-wide risks as nations differ in their application of network and data security. The absence of international norms and standards for information security place all member-states at risk for exploitation.[12] Russia

---

[10] Pezard, Radin, Szayna, and Larrabee, *European Relations*, 16-23.
[11] Susi Dennison, Ulrike Esther Franke, and Paweł Zerka. *The Nightmare of the Dark: The Security Fears that Keep Europeans Up At Night*, European Council on Foreign Relations, July 2018, 1, https://www.ecfr.eu/specials/scorecard/the_nightmare_of_the_dark_the_security_fears_that_keep_europeans_awake_at_n.
[12] Cyberspace Solarium Commission, *Final Report*, 11.

continues to benefit from this lack of alignment within NATO as alliance leaders prefer to squabble over self-interested regional concerns.[13]

Russian meddling is on display election after election as it seeks to unravel the democratic fabric of Europe. There is widespread acknowledgement that Russia is financing multiple political groups within Europe, and forensic attribution places Russian actors at the helm of political influence campaigns in France, Germany, Ukraine, Estonia, Lithuania, Latvia, Poland, and the Republic of Georgia.[14] The Center for Naval Analysis reported in March 2017 on the "pattern of Russia targeting democratic elections… as a means of undermining democratic institutions and the concept of a free electoral process as a whole."[15] Russian agents successfully hacked the 2014 Ukrainian presidential election and discredited the U.S. national election process in 2016.[16] These examples highlight only two instances out of the ninety-one Russian-attributed cyber operations from 2014 through the majority of 2020; however, the Center for Strategic and International Studies (CSIS) reports that nearly half were focused on government or political targets.[17] The Russian threat is only growing bolder and more capable as each hack throughout Europe, and the world, builds credibility, capacity, and doctrine towards further fragmenting the NATO alliance.

(Mis)inform the Masses

Russia targets the voting public of European adversaries through media exploitation to shape public perception, reinforcing the Kremlin's preferred ends. The strength of democratic

---

[13] Dennison, Franke, and Zerka, *The Nightmare of the Dark,* 5.
[14] Center of Strategic and International Studies, "Significant Cyber Incidents," CSIS, accessed 20 September 2020, https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents; Pezard, Radin, Szayna, and Larrabee, *European Relations*, 16-23.
[15] Connell and Vogler, *Russia's Approach,* 24.
[16] Heather A. Conley, "Successfully Countering Russian Election Interference," CSIS, 21 June 2018, https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.
[17] Council on Foreign Relations, "Cyber Operations Tracker," accessed 20 September 2020, https://www.cfr.org/cyber-operations/.

governments lies with their citizens and the power of the polls to drive the direction of national ideology. Russia recognizes this center of gravity and actively seeks to compel the masses through various campaigns of propaganda, misinformation, and ethnic outreach.[18] This tactic complements Russia's ongoing subversive political campaign at the state level and seeks to undo the democratic process from within. The twenty-first century's dependence on social media and instant access to shared information is the medium through which Russian actors spin their narrative, undermining democratic principles and countering the strength of liberal international organizations such as NATO.

Russia sends its message directly to the people through targeted state-controlled media broadcasts, propaganda, and leaks of sensitive information to bolster pro-Russian support while demeaning potential adversaries.[19] State-sponsored "keyboard armies" operating out of organized troll farms attempt "to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space."[20] The pervasive influence of these false reports discredit national media and frustrate government entities as they wrestle for control of the narrative amongst the confusion.

Lines of Effort

The collective resolve of the NATO alliance has not faced a test of this magnitude since the Soviet Union's fall. The common thread among Russia's non-kinetic threats is their delivery through the cyber domain. Russian hybrid warfare is wholly dependent on the cyber domain for its freedom of action and magnified effects from malware to social engineering. NATO must

---

[18] Connell and Vogler, *Russia's Approach*, 25.
[19] Connell and Vogler, *Russia's Approach,* 25.
[20] Sabra Ayres, "Government-controlled 'keyboard' armies now a global phenomenon, new report says," The Los Angeles Times, November 13, 2017, https://www.latimes.com/world/europe/la-fg-internet-freedom-20171113-story.html; Adrian Chen, "The Real Paranoia-Inducing Purpose of Russian Hacks," The New Yorker, July 27, 2016, quoted in Michael Connell and Sarah Vogler, *Russia's Approach to Cyber Warfare*, CNA, March 2017, 26, https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

organize and respond to the threat of hybrid warfare by building a layered structure of capabilities reinforced by overarching strategic goals to guide the principle of defending forward in Europe. Russia uses the cyber domain to enable their application of hybrid warfare tactics to achieve their ends throughout Europe. Therefore, the cyber domain represents the critical requirement of the Russian instability campaign creating an opportunity for NATO to effectively deny or degrade Russia's strategic goals on the continent. Furthermore, EUCOM has a crucial role in enabling and supporting this evolution within NATO's strategic concept.

The recommended reorganization of NATO's posture begins with establishing and defending norms of behavior in the cyber domain. NATO must leverage the power of international law in establishing the moral and ethical high ground from which to apply national power to counter Russian malign acts. The Cyberspace Solarium Commission finds that "maximizing the effectiveness of norms and non-military tools of statecraft leads to a more stable and secure cyberspace."[21] This approach, that can be defined and legitimized in doctrine at the alliance and state level, would be an effective weapon to use as a first layer of defense against cyber-attacks and shape the cyber domain. Additionally, the weight of international law and public perception provides both escalatory and de-escalatory measures to combat malign activities below the level of war while still imposing cost on an adversary and their strategic message. Having achieved legitimacy in the cyber domain, NATO will benefit from freedom of action further along the escalation ladder.

Policy and legitimacy alone will not effectively counter a determined adversary; therefore, NATO must complement its established cyber authority with a surveillance and defense posture relevant and responsive to an ever-changing threat. This approach's overarching

[21] Cyberspace Solarium Commission, *Final Report*, 46.

goal is to mitigate risks to critical infrastructure while passively engaging to understand the threat and adjust network postures accordingly.[22] RAND finds that "NATO needs to quickly catch up by urgently programming warfare development efforts to effectively anticipate adversaries' intentions, disrupt their activities, and provide on-time capabilities to the warfighter."[23] NATO can employ and oversee this capability from its recently established Cyberspace Operations Center, which would serve as the allied citadel of cyber doctrine and lessons learned. However, this concept will rely on the integrated support of all NATO member-states in order to provide the desired layered security effects. The interconnected nature of economies, data networks, and weapons systems require each NATO contributor to establish the same standard of cybersecurity so as not to undermine the alliance through individual vulnerabilities. Furthermore, NATO must build complementary relationships with the private sector to protect critical infrastructure and the public networks on which it relies. Safeguarding the cyber domain is equally beneficial for both public and private investment since both are vulnerable to malign acts; this linkage brings together national capacity with private innovation and expertise ensuring an adequately fused and responsive defense.[24]

A defensive posture is not enough to ensure security in the cyber domain; it requires a deterrent capability.[25] The outer, encapsulating layer of this recommended strategy relies on establishing deterrence through both policy and practice to ensure that NATO retains capability and intent in the cyber domain. NATO has publicly committed to the possibility of an Article Five response to a cyberattack. Unfortunately, NATO does not have the mature cyber capability

---

[22] Cyberspace Solarium Commission, *Final Report*, 4.
[23] Lillian Ablon, Anika Binnendijk, Quentin E. Hodgson, Bilyana Lilly, Sasha Romanosky, David Senty, and Julia A. Thompson, *Operationalizing Cyberspace as a Military Domain: Lessons for NATO*, (Santa Monica, CA: RAND Corporation, 2019), 31, https://www.rand.org/pubs/perspectives/PE329.html.
[24] Ablon, Binnendijk, Hodgson, Lilly, Romanosky, Senty, and Thompson, *Operationalizing Cyberspace,* 21.
[25] Cyberspace Solarium Commission, *Final* Report, 24.

required to address an attack in kind without directly escalating to kinetic action.[26] This lack of options hamstrings NATO's response and defeats the intent of its deterrent message. Therefore, NATO must leverage and build on its cyber-surveillance node to attribute and target cyber threats following any attack or intrusion. Furthermore, defensive and offensive cyber planning and activities must be included in military exercises at every level throughout the alliance. A persistent and robust exercise and simulation campaign will build the much-needed skillset while probing own networks for vulnerabilities. NATO benefits from the diverse resources and expertise of its member-states. The United States, which shepherds a robust cyber warfare enterprise, stands able to mentor and assist a whole-of-NATO approach to this embattled domain.

The Unintended Escalation of an Article Five Response

It could be argued that NATO has overextended its reach in adopting a position that cannot be successfully defended on the international stage. For instance, NATO's application of Article Five to cyber warfare is bereft of the legitimacy of international law, which fails to address sovereignty violations through hybrid means.[27] Additionally, Russia's hybrid activities, focused on influence and exploitation, avoid kinetic effects and preserve the competition continuum.[28] NATO risks an unintended escalation by invoking an Article Five response to a cyber-attack occurring below the level of war as the corresponding lack of precedent and international norms prevent authority and legitimacy in the use of force. Therefore, NATO cannot operate within its cyber doctrine while maintaining legitimacy in adapting to the diverse nature of cyber threats in the twenty-first century. While this argument has merit, it places too

[26] Ablon, Binnendijk, Hodgson, Lilly, Romanosky, Senty, and Thompson, *Operationalizing Cyberspace,* 8.
[27] Cyberspace Solarium Commission, *Final Report*, 18.
[28] Gale A. Mattox, "The Transatlantic Security Landscape in Europe," in *The Oxford Handbook of U.S. National Security*, ed. Nikolas K Gvosdev et al. (New York, NY: Oxford University Press, 2018), 5.

much emphasis on current international law instead of recognizing the role that nations and international organizations play in shaping precedent. Networks across NATO member-states may face challenges, but the value and impact of establishing a rules-based order for cyber-sovereignty is the responsibility of liberal democratic institutions. Furthermore, NATO's investment and leadership in the cyber domain will enable alliance success in countering hybrid warfare.

Enabling Recommendations for EUCOM/SACEUR

The EUCOM Commander, acting also as the Supreme Allied Command (SACEUR) of NATO Forces, can employ various cyber-supportive initiatives to help establish NATO's layered cyber defense posture. EUCOM is effectively poised to "foster a capable and successful workforce, leadership, and command structure for cyberspace operations."[29] First, EUCOM can conduct national engagement with NATO partners in a train and equip role furthering the defensive layer of NATO cyber strategy. EUCOM has a proven construct in its Joint Cyber Center, which can serve as the functional building block of NATO's planned Cyberspace Operations Center. This integration will be vital in providing lessons learned, identifying capability gaps, and connecting resource partners to strengthen the whole of NATO network defense. Additionally, interactions at the military and state level allow for partnerships to develop between the public and private sectors enabling the mutually beneficial exchange of talent and expertise in developing a whole of government and whole of society approach to hardening networks.[30]

The EUCOM/SACEUR role requires both cyber capability and the development of structures necessary to evaluate and ensure operational capacity. Allied forces can easily evolve

[29] Ablon, Binnendijk, Hodgson, Lilly, Romanosky, Senty, and Thompson, *Operationalizing Cyberspace,* 31.
[30] Ablon, Binnendijk, Hodgson, Lilly, Romanosky, Senty, and Thompson, *Operationalizing Cyberspace,* 21.

their current multinational exercise program into joint, coordinated, and comprehensive exercises integrating cyber throughout.[31] This approach allows for the practice of the full application of cyber effects at every level of warfare to train and condition forces to the complementary nature of kinetic and non-kinetic effects. Binational and multinational interactions will develop the corporate knowledge, capability, confidence, and best practices needed to excel in the cyber domain. A comprehensive training and exercise initiative can be coupled with conferences focused on state and military actors such as the Program on Cyber Security Studies at the Marshall Center in providing member-state education and alignment throughout the region.[32] However, this exchange of ideas must attack NATO's most critical cyber capability gap: individual talent at the operational and tactical levels.[33] NATO can ensure longstanding success and dominance by resourcing its need for a modern cyber workforce.[34]

Partnerships with the private sector will continually benefit NATO and EUCOM cyber operations; however, there is much to be gained through enmeshing the pillars of academia to address the cyber threat. For example, EUCOM could establish an internship through the U.S. Department of State to allow for vetted cybersecurity students and professionals to join a NATO response team or support operations at the Cyber Operations Center to build a workforce from the ground up. NATO must build a cyberculture and capability that seamlessly integrates across nations and throughout the public and private sectors. Incorporating academia and civilian talent

---

[31] Ablon, Binnendijk, Hodgson, Lilly, Romanosky, Senty, and Thompson, *Operationalizing Cyberspace,* 2.
[32] Christine June, "Marshall Center Program Engages Experts to Address Challenges, Threats in Cyberspace," George C. Marshall European Center for Security Studies, 27 December 2018, https://www.army.mil/article/215505/marshall_center_program_engages_experts_to_address_challenges_threats_in_cyberspace.
[33] Ablon, Binnendijk, Hodgson, Lilly, Romanosky, Senty, and Thompson, *Operationalizing Cyberspace, 2.*
[34] Ablon, Binnendijk, Hodgson, Lilly, Romanosky, Senty, and Thompson, *Operationalizing Cyberspace,* 15-16.

ensures a comprehensive approach and complements innovation to defend European networks from malign acts.[35]

Conclusion

Russian state and non-state actors have masterminded hybrid activity throughout Europe over the past decade; they have stolen from, influenced, and crippled public and private institutions alike while cloaked in anonymity and deceit. The time has come for NATO to unite under the umbrella of its liberal democratic roots to combat Russia's escalatory hybrid campaign across Europe and, in doing so, find alignment and unity among member-states.

NATO's success in the Cold War was a result of its strength as a multinational network of systems, sensors, and capabilities that, when combined, produced a deterrent united by the principle of collective defense. This model still stands today and is the backbone on which NATO must evolve to defend its interests and intellectual property against malign Russian acts. Once again, NATO has the opportunity to advance the free world through a time of conflict and uncertainty by ensuring that liberal ideals define the standards of both cyber conduct and hybrid warfare. In the face of the growing cyber assault, NATO's pivot and affirmation of Article Five in response to cyber-attacks set Europe and the world on a new path to peace through strength.[36] Ultimately, the promise and deterrent of NATO solidarity, backed by EUCOM, is the crucial weapon needed to counter and defeat Russian malign hybrid activity.

---

[35] Ablon, Binnendijk, Hodgson, Lilly, Romanosky, Senty, and Thompson, *Operationalizing Cyberspace,* 16.
[36] Paul Belkin, *NATO: Key Issues Following the 2019 Leaders' Meeting*, CRS, Updated 1 April 2020, https://www.everycrsreport.com/reports/R46066.html; North Atlantic Treaty Organization, "NATO Will Defend Itself," NATO, 29 August 2019, https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en.

Bibliography

Ablon, Lillian, Anika Binnendijk, Quentin E. Hodgson, Bilyana Lilly, Sasha Romanosky, David Senty, and Julia A. Thompson. *Operationalizing Cyberspace as a Military Domain: Lessons for NATO.* Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/perspectives/PE329.html.

Ayres, Sabra. "Government-controlled 'keyboard' armies now a global phenomenon, new report says." *The Los Angeles Times*, November 13, 2017. https://www.latimes.com/world/europe/la-fg-internet-freedom-20171113-story.html.

Belkin, Paul. *NATO: Key Issues Following the 2019 Leaders' Meeting*. CRS, Updated 1 April 2020. https://www.everycrsreport.com/reports/R46066.html.

Center of Strategic and International Studies. "Significant Cyber Incidents." CSIS, accessed 20 September 2020. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

Cerulus, Laurens. "How Ukraine became a test bed for cyberweaponry." *Politico*, 14 February 2019. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

Chen, Adrian. "The Real Paranoia-Inducing Purpose of Russian Hacks." The New Yorker, July 27, 2016. Quoted in Michael Connell and Sarah Vogler. *Russia's Approach to Cyber Warfare*. CNA, March 2017. 26. https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

Conley, Heather A. "Successfully Countering Russian Election Interference." CSIS, 21 June 2018. https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.

Connell, Michael and Sarah Vogler. *Russia's Approach to Cyber Warfare.* CNA, March 2017. https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

Council on Foreign Relations. "Cyber Operations Tracker." CFR, accessed 20 September 2020. https://www.cfr.org/cyber-operations/.

Cyberspace Solarium Commission. *Final Report*. March 2020. https://www.solarium.gov/report.

Dennison, Susi, Ulrike Esther Franke, and Paweł Zerka. *The Nightmare of the Dark: The Security Fears that Keep Europeans Up At Night.* European Council on Foreign Relations, July 2018. https://www.ecfr.eu/specials/scorecard/the_nightmare_of_the_dark_the_security_fears_that_keep_europeans_awake_at_n.

June, Christine. "Marshall Center Program Engages Experts to Address Challenges, Threats in Cyberspace." George C. Marshall European Center for Security Studies, 27 December 2018. https://www.army.mil/article/215505/marshall_center_program_engages_experts_to_address_challenges_threats_in_cyberspace.

Mattox, Gale A. "The Transatlantic Security Landscape in Europe." Chap. 32 in The Oxford Handbook of U.S. National Security. Edited by Nikolas K Gvosdev, Derek S. Reveron, and John A. Cloud. New York, NY: Oxford University Press, 2018.

Mazarr, Michael, Jonathan S. Blake, Abigail Casey, Tim McDonald, Stephanie Pezard, and Michael Spirtas. *Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives*. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR2726.html.

National Counterintelligence and Security Center. *Economic Espionage Counter Intel and Security.* 2018, pp. 1-15. https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

North Atlantic Treaty Organization. "NATO Will Defend Itself." NATO, 29 August 2019, https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en.

Pezard, Stephanie, Andrew Radin, Thomas S. Szayna, and F. Stephen Larrabee. *European Relations with Russia: Threat Perceptions, Responses, and Strategies in the Wake of the Ukrainian Crisis*. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1579.html.