alliance for securing democracy
G|M|F

Policy Brief

2018 | No. 031

NATO and Asymmetric Threats: A Blueprint for Defense and Deterrence

By Brittany Beaulieu and David Salvo

Russia is increasingly turning its asymmetric arsenal on NATO allies to attack the credibility of the Alliance, undermine democratic institutions across member states, and disrupt NATO cohesion on a variety of policy and security issues. Despite falling below the threshold of conventional warfare, asymmetric threats are designed to weaken the security of the Alliance and individual allies, as well as destabilize allied governments and societies. NATO has taken some measures to address hybrid threats; however, NATO needs a more comprehensive strategy to counter the growing threat that asymmetric interference poses. The NATO Brussels Summit taking place July 11 and 12 presents an important opportunity on this front.

To better position itself to tackle these challenges, the Alliance should: (1) elevate discussion of hybrid threats in the North Atlantic Council (NAC), permit allies to invoke Article 4 when confronted with hybrid threats to share information and request assistance through hybrid response teams, and internally clarify thresholds for coordinated response in times of hybrid crises; (2) work with NATO allies and with the EU to ensure the optimal utilization of resources and expertise in combating asymmetric threats; (3) develop stronger public-private partnerships to address asymmetric threats outside the purview of the Alliance; (4) invest in resources to improve resilience in individual member states, as mandated by Article 3; and (5) issue a declaratory statement that hybrid, asymmetric tactics pose a serious threat to the Alliance and that allies will respond appropriately.

Asymmetric Attacks on the Alliance

The Alliance defines hybrid threats as "combin[ing] military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of targets." Russia's three-week cyber-attack on Estonia in 2007, along with its annexation of Crimea and invasion of eastern Ukraine in 2014 using hybrid tactics in conjunction with conventional warfare, and the potential implications for NATO allies like the Baltic states, elevated the issue on the Alliance's agenda.

NATO allies have been increasingly targeted by these asymmetric tools of interference. Russia's operation against the 2016 U.S. presidential election, along with interference in elections and referendums in France,[1] Montenegro,[2] the Czech Republic,[3] the

1 Michel Rose and Denis Dyomkin, "After Talks, France's Macron Hits Out at Russian Media, Putin Denies Hacking," *Reuters*, May 28, 2017; Andrew Roth and James McAuley, "Russian Media Leap on French Presidential Candidate with Rumors and Innuendo," *Washington Post*, Feb. 6, 2017; Richard Balmforth and Michel Rose, "French Polling Watchdog Warns over Russian News Agency's Election Report," *Reuters*, April 2, 2017.

2 Jonathan Keane, "Hackers Tried to Disrupt the Parliamentary Elections in Montenegro," *Business Insider*, Oct. 17, 2016.

3 Markéta Krejčí, Veronika Víchová, and Jakub Janda, "The Role of the Kremlin's Influence and Disinformation in the Czech Presidential Elections," *European Values*, Jan. 29, 2018 http://www.europeanvalues.net/wp-content/uploads/2018/02/The-role-of-the-Kremlin%E2%80%99s-influence-and-disinformation-in-the-Czech-presidential-elections.pdf.

United Kingdom,[4] and Spain,[5] among others, have highlighted the risks to allies' security even through unconventional tools and tactics. These same tactics have targeted government institutions,[6] political parties,[7] and even NATO itself.[8]

Indeed, NATO is frequently the target of Russian disinformation. For example, in 2017, a disinformation campaign widely believed to have originated in Russia[9] falsely alleged that German soldiers deployed in Lithuania had raped a teenage girl. This followed false allegations of allied soldiers' "bad behavior,"[10] including the unsubstantiated claim that allied soldiers would wander the Latvian countryside with loaded weapons. As one of the myriad of conspiracy theories Russian state media propagated to explain away the Russian government's poisoning of Sergei and Yulia Skripal in the U.K., official Russian media outlet Sputnik spuriously claimed NATO plotted the attack in order to justify increased defense spending.[11] In NATO partner countries, such as Sweden, Georgia, and Ukraine, Russian disinformation seeks to malign NATO and undermine citizens' support for joining the Alliance.[12] And Russian-linked accounts tracked by the Hamilton 68 dashboard promote narratives to an American audience that portray a Europe in chaos, including criticism and false allegations directed at the EU and NATO.

Russia also employs cyber capabilities to target political parties, candidates, and government institutions in an effort to attain compromising information. Fancy Bear and Cozy Bear, both linked to Russia's Main Intelligence Directorate, hacked the Democratic National Committee and Clinton campaign officials' email accounts during the 2016 U.S. presidential election,[13] attaining information that it fed to its proxy WikiLeaks in the critical months before election day.[14] In France, the same group hacked the Macron campaign,[15] and in Germany, it accessed internal servers of the Bundestag and the federal government's networks.[16]

Russia employs cyber capabilities to target political parties, candidates, and government institutions."

In addition to disinformation and cyber-attacks, Russian and other state actors also provide overt and covert support for political and social groups, such as the €11 million loan from Kremlin-linked First Czech Russian Bank to France's far-right National Front in 2014,[17] and the cooperation agreements the United Russia party has signed with other Eurosceptic parties, Italy's Lega Nord and Austria's Freedom Party.[18] It also supports a network of government-organized nongovervnmental organizations, or GONGOs, throughout Europe whose objective is to "shift European public opinion toward a positive view of Russian politics and policies, and toward respect

4 Iggy Ostanin and Elanenor Rose, "Brexit: How Russian Influence Undermines Public Trust in Referendums," *Organized Crime and Reporting Project*, June 20, 2016, https://www.occrp.org/en/investigations/5368-brexit-how-russian-influence-undermines-public-trust-in-referendums/.

5 Robin Emmott, "Spain Sees Russian Interference in Catalonia Separatist Vote," *Reuters*, Nov. 13, 2017.

6 "Norway Accuses Group Linked to Russia of Carrying Out Cyber-Attack," *The Guardian*, Feb. 3, 2017.

7 Feike Hacquebord, "Pawn Storm Targets German Christian Democratic Union," Trend Micro, May 11, 2016, https://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-targets-german-christian-democratic-union/.

8 "NATO: Russia Targeted German Army With Fake News Campaign," *Deutsche Welle*, Feb 16, 2017, http://www.dw.com/en/nato-russia-targeted-german-army-with-fake-news-campaign/a-37591978.

9 "Why the 'Fake Rape' Story Against German NATO Forces Fell Flat in Lithuania," *Deutsche Welle*, Feb. 23, 2017.

10 Marta Kepe, "NATO: Prepared for Countering Disinformation Operations in the Baltic States?" RAND Corp, June 6, 2017, https://www.rand.org/blog/2017/06/nato-prepared-for-countering-disinformation-operations.html.

11 "NATO Plotted 'Skripal Case' to Justify Their Defense Spendings — Moscow," Sputnik, April, 3, 2018, https://sputniknews.com/europe/201804031063159491-nato-not-issue-visas-russian-diplomats/.

12 Brittany Beaulieu and Steven Keil, "Russia as Spoiler: Projecting Division in Transatlantic Societies," Alliance for Securing Democracy, June 19, 2018, https://securingdemocracy.gmfus.org/russia-as-spoiler-projecting-division-in-transatlantic-societies/.

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

14 Patrick Tucker and Defense One, "Was Russia Behind the DNC Hack?" The Atlantic, July 25, 2016.

15 Eric Auchard, "Macron Campaign Was Target of Cyber Attacks by Spy-Linked Group," *Reuters*, April 24, 2017.

16 "Fancy Bear: Germany Investigates Cyber-Attack 'by Russians,'" *BBC*, February 28, 2018.

17 Gabriel Gatehouse, "Marine Le Pen: Who's Funding France's Far Right?" *BBC*, April 3, 2017.

18 Damien Sharkov, "Russia's Ruling Party Strikes Cooperation Deal With Italian Euroskeptics," *Newsweek*, June 3, 2017.

for its great power ambitions."[19] Russia also invests in energy and key industrial sectors to acquire political and economic leverage and exploits financial systems and institutionalizes corruption in order to weaken democratic institutions in NATO member states.[20]

NATO's Response

NATO's Comprehensive Approach Action Plan, adopted at the 2008 Bucharest Summit[21] and reaffirmed at the 2010 Lisbon Summit,[22] laid the framework for mobilizing military, political, and civilian resources to jointly address crisis situations, which was a positive recognition of the hybrid challenge and a good first step to address it. A more substantial development in the cyber realm was reflected in the Wales Summit Declaration[23] in 2014, when NATO declared that cyber-attacks could lead to invocation of Article 5 of the Washington Treaty.[24]

At the December 2015 NATO Foreign Ministerial meeting, NATO adopted a strategy for confronting hybrid threats and pledged greater cooperation with the EU in doing so.[25] Part of this included better information-sharing and early warning of hybrid threats from both the East and the South. Member states were also encouraged to map potential vulnerabilities to Russian influence in "business, financial, media or energy concerns" and share best practices and lessons learned in building resilience within NATO.[26] At the 2016 Warsaw Summit, NATO took another step toward greater cooperation with the EU when it agreed on a strategy for Countering Hybrid Warfare that it is implementing in coordination with the EU.[27] And much like the EU counters Russian disinformation through its East StratCom Task Force, NATO's public diplomacy office employs the #WeAreNATO hashtag to counter anti-NATO narratives.[28]

NATO has also taken a leading role in deepening analysis of these threats and facilitating development of potential responses. NATO established Centers of Excellence to analyze and develop strategies to respond to individual elements of the asymmetric toolkit, such as the Cooperative Cyber Defense Center in Estonia and the Strategic Communications Center of Excellence in Latvia. NATO also contributed to the establishment of the European Center of Excellence for Countering Hybrid Threats in Finland that originated with the EU's 2016 "Joint Framework on countering hybrid threats"[29] and was further supported in the "Common set of proposals for the implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization, which works across the EU and NATO."[30] The Center coordinates the activity of the EU Hybrid Fusion Cell and relevant NATO counterparts in the development of "comprehensive, whole-of-government" responses to hybrid, asymmetric threats.[31] These centers allow

NATO has taken a leading role in deepening analysis of hybrid threats and facilitating development of potential responses."

19 Vladka Vojtiskova, Hubertus Schmid-Schmidsfelden, Vít Novotny, and Kristina Potapova, "The Bear in Sheep's "Clothing: Russia's Government-Funded Organisations in the EU," Wilfried Martins Center for European Studies, July 2016.

20 Heather Conley, "The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe," Center for Strategic and International Studies, October 13, 2016.

21 "Bucharest Summit Declaration," North Atlantic Treaty Organization, April 3, 2008, https://www.nato.int/cps/en/natohq/official_texts_8443.htm.

22 "Lisbon Summit Declaration," North Atlantic Treaty Organization, November 20, 2010 https://www.nato.int/cps/en/natohq/official_texts_68828.htm.

23 "Whales Summit Declaration," North Atlantic Treaty Organization, September 5, 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

24 Ibid.

25 Jens Stoltenberg and Federica Mogherini, "Press Statements," North Atlantic Treaty Organization, December 2, 2015, www.nato.int/cps/en/natohq/opinions_125361.htm.

26 "Resilience: A Core Element of Collective Defense," *North Atlantic Treaty Organization,* https://www.nato.int/docu/review/2016/also-in-2016/nato-defence-cyber-resilience/en/index.htm.

27 Federico Yaniz, "Projecting Stability: Hybrid Warfare and Cooperation With the EU," Atlantic Treaty Association, February 2, 2018, http://www.atahq.org/2018/02/projecting-stability-hybrid-warfare-cooperation-eu/.

28 Julianne Smith, Jim Townsend, and Rachel Rizzo, "NATO's 2018 Summit: Key Summit Deliverables and Five Initiatives Where the U.S. Can Make a Difference," Center for a New American Security, March 30, 2018, https://www.cnas.org/publications/reports/natos-2018-summit.

29 "Joint Framework on Countering Hybrid Threats," European Commission, June 4, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018.

30 "Common set of proposals for the implementation of the Joint Declaration," The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/wp-content/uploads/2017/08/Common-set-of-proposals-for-the-implementation-of-the-Joint-Declaration-2.pdf.

31 "About Us," The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/about-us/.

for the sharing of lessons learned and best practices and provide "expertise and experience" to the Alliance on building resilience.[32] However, member state participation in these centers is voluntary and there is no mechanism for mandating member states institutionalize their recommendations. For example, only 16 countries currently participate in the European Center of Excellence for Countering Hybrid Threats. These centers are also removed from policy discussions and meaningful decision-making structures in Brussels and in individual member states.

NATO issued a new communique on its approach to hybrid threats on June 26, 2018, citing an increase in "their speed, scale, and intensity, facilitated by rapid technological change and global interconnectivity." This strategy is based on preparedness, deterrence, and defense, and focuses on the role of the Joint Intelligence and Security Division at NATO Headquarters to improve the Alliance's "understanding and analysis of hybrid threats." It also confers on member states the role of identifying national vulnerabilities and strengthening their own resilience.[33]

Challenges to a Unified Response

While NATO and the EU have pledged to improve their information sharing and coordination of responses across the asymmetric toolkit, these efforts are under-funded and lack high-level coordination. Moreover, the absence of a mechanism to share NATO classified information with the EU, an old problem, prevents both organizations from more systematic cooperation in responding jointly to the hybrid challenge. The lack of information sharing among allies at NATO is another challenge. For example, the United States did not share much information about the Russian operation against the 2016 presidential election as it unfolded and only a meager amount afterward. In the lead up to the French and German elections, information was shared on a bilateral basis, rather than through the NAC. The reservations of some allies to discuss their own vulnerabilities to interference operations only exacerbate NATO's organizational impediments to addressing hybrid threats in a timely and coordinated manner. A formalized information sharing or early warning mechanism could help to rectify this problem, as would decisions in allied capitals to elevate discussion on hybrid threats at the NAC and share more threat information and intelligence.

An inhibitor of NATO's response to emerging asymmetric threats is the differing threat perceptions held by various actors within the Alliance."

There is also a lack of internal clarity regarding how the Alliance will respond to hybrid activities. As the *NATO Review* explains, "in practice, any threat can be hybrid as long as it is not limited to a single form and dimension of warfare. When any threat or use of force is defined as hybrid, the term loses its value and causes confusion instead of clarifying the 'reality' of modern warfare."[34] The reality of modern warfare is that all wars involve hybrid tools and tactics. Furthermore, hybrid threats materialize even in the absence of conventional war, as demonstrated countless times by Russian operations across Europe and the United States over the past decade. This reality is all the more reason for NATO to develop an internal framework for addressing hybrid, asymmetric activities that currently fall below the Article 5 threshold and clearly articulate this framework to allies.

A final inhibitor of NATO's response to emerging asymmetric threats is the differing threat perceptions held by various actors within the Alliance. While those on NATO's eastern frontier have long called for an increased focus on the Kremlin's asymmetric toolkit, the threat of authoritarian interference is less salient to other allies. Much as the United States, France, and the U.K. failed to heed warnings from NATO's Central and East European members about the rise of asymmetric interference years ago, some allies remain unconvinced of the threat. However,

32 "Centres of Excellence," North American Treaty Organization, August 26, 2016, https://www.nato.int/cps/en/natolive/topics_68372.htm.

33 "NATO's Response to Hybrid Threats," North American Treaty Organization, June 26, 2018, https://www.nato.int/cps/en/natohq/topics_156338.htm?.

34 Damien Van Puyvelde, "Hybrid War — Does it Even Exist?" *NATO Review Magazine*.

the growth and spread of these methods presents a challenge to the sovereignty of each and every NATO member and to the unity of the Alliance as a whole. These differing threat perceptions are precisely why allies need to be more vocal about raising the hybrid challenge at more senior levels and more willing to share information in order to build consensus on the threats and alliance responses to them.

Recommendations

1. Allies should invoke Article 4 in response to hybrid threats.

Invoking Article 4 would mandate political consultations to develop political solutions to hybrid attacks. It would provide an opportunity for allies with differing threat perceptions to share intelligence and best practices to reach consensus about deterrent and defensive strategies to combat hybrid threats during crises. These consultations would include discussion of internal thresholds for triggering various responses by the Alliance to hybrid operations, including the invocation of Article 5. They could also facilitate requests by individual allies for support from NATO in responding to a hybrid operation; a NATO-wide hybrid response team should be established to deploy in response to allies' requests.

2. NATO and the EU should institute a Joint Task Force on Countering Asymmetric Threats.

NATO and the EU should further improve collaboration to increase transatlantic resiliency to asymmetric tactics. Each organization has disparate elements that address individual asymmetric tools, but are not all well-funded or in sync with one another's efforts. A Joint Task Force, led by senior officials from both organizations, could better coordinate the work of the various parts of NATO and EU bureaucracies already addressing this challenge to defend against a threat that crosses organizational jurisdictions. Moreover, the Task Force could monitor disinformation campaigns and coordinate public outreach on behalf of both organizations to advocate for the benefits of the transatlantic community in the face of efforts by Russia, China, and others to sell an alternative model for government and society.

3. NATO should further develop public-private partnerships with civil society.

NATO should increase its efforts to develop partnerships with local civil society organizations that can combat disinformation, play the role of the "watch dog" in holding political elites to standards of transparency, and advocate for democratic ideals and principles at the grassroots level. It should also devote additional resources to public diplomacy campaigns, such as the #WeAreNATO campaign, and engage all member states in their coordination. New campaigns could target citizens in rural areas who do not use Facebook or Twitter by engaging them at schools, libraries, and community and retirement centers.

4. Allies should reinvigorate Article 3 — Resiliency

Much of the work to counter malign foreign interference in democracies requires strengthening member states institutions and societies to make them more resilient to these attacks. Under Article 3 of the Washington Treaty, each member state is obligated to "maintain and develop" its "capacity to resist armed attack,"[35] which should include enhancing resilience and civil preparedness in the realms of cybersecurity, energy security, and election security.[36] NATO should renew its focus on Article 3 of the NATO charter and define minimum standards for resilience with a verification process that does not rely on self-reporting. Such an approach is necessary for "21st century defense and deterrence."[37] Member and partner states on the frontline of this assault should receive additional assistance from NATO in order to address persistent vulnerabilities.

5. NATO should issue a declaratory statement.

Hybrid, asymmetric tactics pose a serious threat to the stability of the Alliance and its member states. NATO allies should take the opportunity of the

35 "The North Atlantic Treaty (1949)," North Atlantic Treaty Organization, April 4, 1949, https://www.nato.int/nato_static/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf.

36 Former U.S. Ambassador to NATO and retired Lieutenant General Doug Lute has proposed this idea. Private discussion at the Aspen Strategy Group, June 21, 2018. Cited with permission.

37 Ibid.

Brussels Summit to issue a declaratory statement about the severity of the threat and allies' commitment to appropriately respond to it.

Conclusion

NATO must adapt to confront the challenge of 21st century hybrid, asymmetric threats in order to defend itself against unconventional threats and sustain internal cohesion. While the Alliance has taken steps to address the new threat environment, this challenge cannot be dealt with as primarily a strategic communications exercise or through the development of Centers of Excellence that do not have the ability to institutionalize recommendations. Ensuring robust discussion of hybrid challenges at the upcoming NATO Summit, and adopting measures to refine existing policies and improve coordination with the EU and external actors, would boost NATO's capabilities to defend the Alliance against comprehensive malign foreign interference. Finally, each NATO ally will need to take greater responsibility to build resilience within its own society to protect its security and sovereignty.

The views expressed in GMF publications and commentary are the views of the author alone.

About the Authors

David Salvo is deputy director of the Alliance for Securing Democracy at The German Marshall Fund of the United States.

Brittany Beaulieu is a fellow and program officer at the Alliance for Securing Democracy at The German Marshall Fund of the United States.

About the Alliance for Securing Democracy

The Alliance for Securing Democracy is a bipartisan, transatlantic initiative housed at The German Marshall Fund of the United States (GMF) that is committed to developing comprehensive strategies to defend against, deter, and raise the costs on Russian and other state actors' efforts to undermine democracy and democratic institutions. The Alliance is informed by a bipartisan, transatlantic advisory council composed of former senior officials with experience in politics, foreign policy, intelligence, Russia, and Europe — bringing deep expertise across a range of issues and political perspectives.

About GMF

The German Marshall Fund of the United States (GMF) strengthens transatlantic cooperation on regional, national, and global challenges and opportunities in the spirit of the Marshall Plan. GMF does this by supporting individuals and institutions working in the transatlantic sphere, by convening leaders and members of the policy and business communities, by contributing research and analysis on transatlantic topics, and by providing exchange opportunities to foster renewed commitment to the transatlantic relationship. In addition, GMF supports a number of initiatives to strengthen democracies. Founded in 1972 as a non-partisan, nonprofit organization through a gift from Germany as a permanent memorial to Marshall Plan assistance, GMF maintains a strong presence on both sides of the Atlantic. In addition to its headquarters in Washington, DC, GMF has offices in Berlin, Paris, Brussels, Belgrade, Ankara, Bucharest, and Warsaw. GMF also has smaller representations in Bratislava, Turin, and Stockholm.

1700 18th Street NW
Washington, DC 20009
T 1 202 683 2650 | F 1 202 265 1662 | E info@gmfus.org
http://www.securingdemocracy.org/