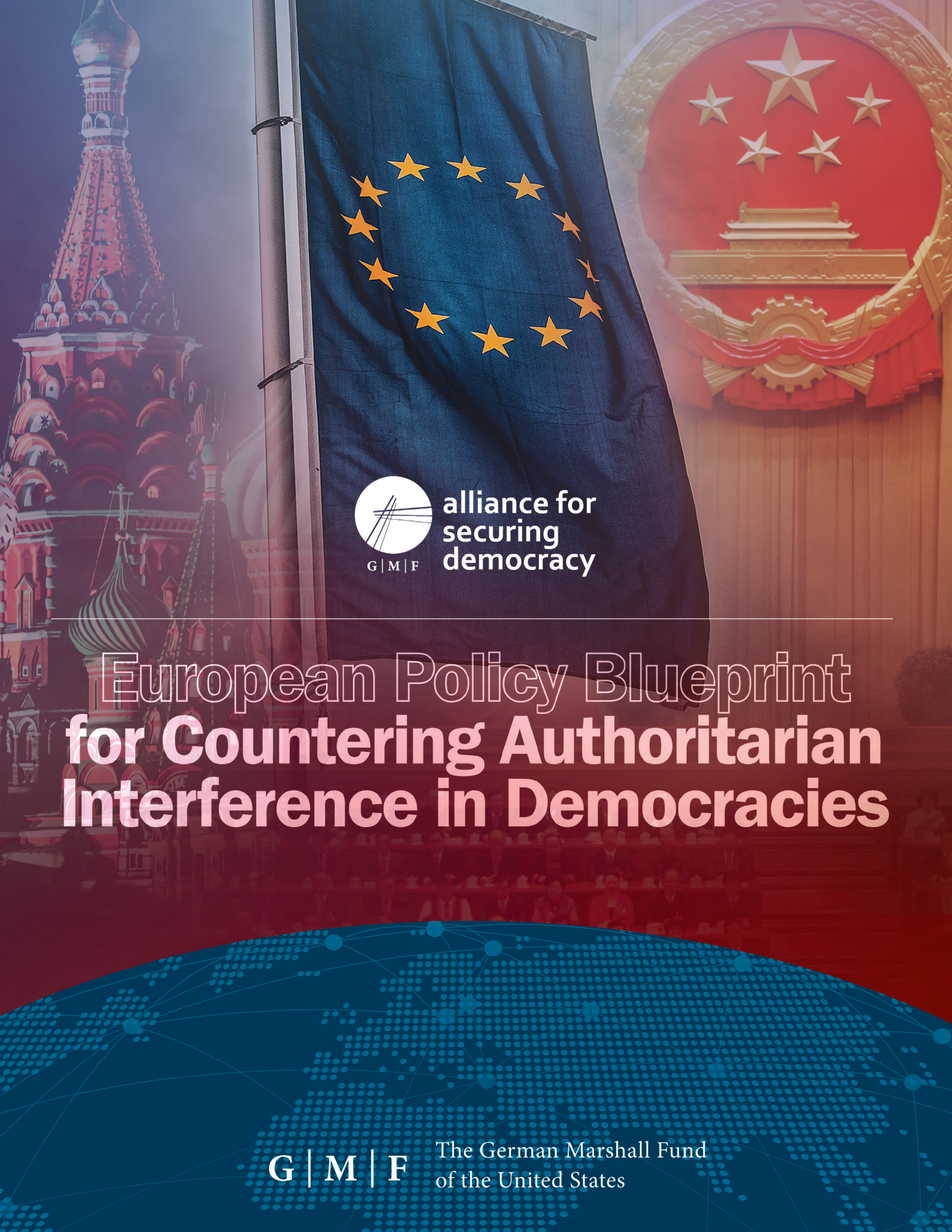

alliance for securing democracy

G|M|F

European Policy Blueprint for Countering Authoritarian Interference in Democracies

G|M|F The German Marshall Fund of the United States

Please direct inquiries to
The Alliance for Securing Democracy at
The German Marshall Fund of the United States
1744 R Street, NW
Washington, DC 20009
T 1 202 683 2650
F 1 202 265 1662
E info@securingdemocracy.org

This publication can be downloaded for free at http://www.gmfus.org/listings/research/type/publication.

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 contributes research and analysis and convenes leaders on transatlantic issues relevant to policymakers. GMF offers rising leaders opportunities to develop their skills and networks through transatlantic exchange, and supports civil society in the Balkans and Black Sea regions by fostering democratic initiatives, rule of law, and regional cooperation. Founded in 1972 as a non-partisan, non-profit 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.

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 the authors

Kristine Berzina is a senior fellow at the Alliance for Securing Democracy

Dr. Nad'a Kovalcikova is a fellow and program manager, European outreach, at the Alliance for Securing Democracy

David Salvo is the deputy director of the Alliance for Securing Democracy and a senior fellow at the German Marshall Fund of the United States

Etienne Soula is a research assistant at the Alliance for Securing Democracy

EUROPEAN POLICY BLUEPRINT FOR COUNTERING AUTHORITARIAN INTERFERENCE IN DEMOCRACIES

2019 | No. 18

KRISTINE BERZINA, NAD'A KOVALCIKOVA, DAVID SALVO, AND ETIENNE SOULA

EXECUTIVE SUMMARY

In recent years, European democracy has been shaken by internal and external events. European nations and institutions are confronting numerous challenges like migration, nationalist extremism, and discontent with the political status quo. They also face challenges from a revanchist Russia that seeks to reestablish influence it lost after the collapse of the Soviet Union and to weaken democracy across the continent, and from a rising China that aims to export its model of authoritarianism across the globe. The European Union and NATO have expanded their membership, bringing more European citizens into the Euro-Atlantic community, and yet a polarized European society remains ever more susceptible to interference from foreign authoritarian regimes' attempts to undermine Europe's stability, unity, and prosperity.

The overall security threat to Europe has evolved. Europe's adversaries are less likely to use conventional military power to fight today's geopolitical battles and more likely to employ asymmetric tools to compensate for conventional military weaknesses—cyberattacks, information operations, malign financial influence, the subversion of political and social organizations, and strategic economic coercion. Regimes like Vladimir Putin's Russia amplify divisive narratives to undermine public trust in democracy using a combination of state-controlled media outlets, government-sponsored online trolls masquerading as European citizens, and a network of sympathetic social media agitators. Authoritarian actors bring money into Europe licitly and illicitly to corrupt European leaders and peddle their influence in European politics and society. They use state assets as leverage to create economic dependencies that further authoritarian interests in Europe and advance their corroding influence across the continent. Finally, these regimes disrupt democracies' ability to govern and function by conducting cyberattacks against government institutions, businesses, and media.

> *"A polarized European society remains ever more susceptible to interference from foreign authoritarian regimes' attempts to undermine Europe's stability, unity, and prosperity.*

Elections are a prime target of authoritarian attacks on democracy. The Russian government has interfered in elections and referendums in several European nations, and initial assessments of the May 2019 European Parliament elections revealed that Russian disinformation campaigns "covered a broad range of topics" to attack the EU, amplify localized polarizing content to influence public opinion, and attempt to suppress voter turnout.[1] But undermining elections is not the only goal. Authoritarian incursions into the daily lives of Europeans have increased since the Russian invasion of Crimea in 2014, and they will grow by an order of magnitude as technologies evolve and

1 High Representative of the Union for Foreign Affairs and Security Policy, "Report on the Implementation of the Action Plan Against Disinformation," European Commission, June 14, 2019.

more actors adopt these tools. By using these tools to exploit existing cleavages in democratic societies and vulnerabilities in democratic governments, authoritarian regimes are trying to weaken and distract Europe and its transatlantic partners in the United States and Canada from their regional and global responsibilities, and to diminish confidence in democracy as a viable form of government.

A New Strategic Approach for Europe

Europe has been a leader in addressing the authoritarian interference threat. Long before the United States acknowledged the threat, European institutions and several European governments had already mobilized to defend against it. The EU and NATO launched task forces and centers of excellence that analyze authoritarian tools and tactics; nations like Sweden assigned responsibility in coordinating efforts to respond to this challenge to a particular government agency; and civil society initiatives all over Europe emerged to monitor and analyze foreign interference operations in their own countries. Yet vulnerabilities to authoritarian interference persist across the continent—in governments, institutions, and society. Despite a burgeoning of initiatives to confront this challenge, many are hampered by a lack of resources, coordination, and top-level political support. Some nations have hardly dealt with their vulnerabilities at all, and just as troubling is the courtship of authoritarian actors by some national leaders for their own political gain. The interaction between governments and other key players in democracy, particularly civil society and the private sector, has been limited.

For Europe to succeed, it needs continent-wide buy-in on a new strategic approach to tackling the authoritarian interference challenge—one that involves whole-of-government and whole-of-society efforts. Working with transatlantic and other democratic partners around the globe, European nations and institutions must harness their combined political weight to identify and develop defensive measures against foreign interference, and to raise the cost of conducting operations against their citizens. Tech and social media companies, whose platforms authoritarian regimes exploit to the detriment of democracy, must improve transparency, information sharing, and their corporate policies to secure the digital information space. Traditional media organizations should adopt norms and guidelines for ethical reporting in the disinformation era, and independent and local journalism must be better supported. And civil society should continue to raise awareness about the foreign interference challenge and develop tools to build resilience in society, including media and digital literacy programs.

> *"Europe has been a leader in addressing the authoritarian interference threat across the continent—in governments, institutions, and society.*

Recommendations

This report identifies specific, actionable recommendations for EU institutions, NATO, national governments, the private sector, the media, and civil society to defend against the authoritarian interference challenge in a more coordinated, sustained, and strategic manner. The recommendations build toward the following ten main principles.

1. Improve coordination to develop collective responses to foreign interference operations

There are many efforts underway nationally and at the EU and NATO level to defend against authoritarian interference. However, some efforts are not well coordinated organizationally and do not always feed into decision-making structures. National governments should centralize mechanisms for tracking and analyzing threats and developing policy responses. The EU should institute a senior-level coordinator for interference issues to oversee various efforts across EU institutions and facilitate the sharing of best practices by member states.

EU-NATO cooperation on hybrid threats should be strengthened by having more formal consultations at the heads of state and government level, and by implementing thoroughly agreed measures from EU-NATO joint declarations.

2. Protect the principles and institutions of democracy, remembering that our democracy is only as strong as we make it

European citizens have a responsibility to protect themselves and their societies from interference by holding governments and businesses accountable, and actively participating in political processes and civil society. Whole-of society resilience is critical as evolving technology is expected to enable an already growing number of foreign authoritarian actors to engage in increasingly sophisticated manners of interference. Maintaining the rule of law, protecting the freedom of speech, and fighting corruption at all levels is paramount to inoculating society against authoritarian incursions.

3. Raise the cost of interference in Europe

Authoritarian governments that engage in interference operations must know that the repercussions for doing so will be costly and sustained. European states should maintain intra-European as well as transatlantic unity on existing sanctions and expand them if malign foreign actors further target European democracies, and they should adopt other financial and reputational countermeasures as necessary. NATO should further articulate what hybrid activity it considers a threat to the national security of allies and clarify publicly how it intends to harness alliance capabilities to defend allies from these attacks.

4. Continue to push for transparency and accountability in the information and technology sectors

The efforts of tech platforms to counter foreign interference operations have at times been opaque and their policies inconsistently applied. European governments and institutions should keep working with the platforms to encourage maximum transparency about their policies to protect rights to user data and stymie malicious actors. At the same time, they must be careful not to impair user anonymity, which can protect democratic actors. Social media companies should improve the transparency of political ad funding and targeting, ensure that government-sponsored content and accounts are labeled properly, define and label social bots, and increase information sharing with independent researchers, governments, and among each other regarding removed accounts and specific threats.

5. Build more constructive public-private partnerships to identify and address evolving digital threats

Threats in the online information space and in cyberspace evolve constantly. European governments, media, and the private sector need to work together to share best practices and tools for building better media literacy, detecting hostile information operations, identifying bad actors and false content, and communicating threats to the public. The EU Code of Practice on Disinformation is an ambitious initial approach that needs to be enhanced by addressing smaller platforms, encouraging cross-platform information sharing, and ensuring that signatories thoroughly deliver and meaningfully report on progress against disinformation as they pledged.

6. Tackle entrenched vulnerabilities in the financial sector that authoritarian actors exploit

Abetted by local enablers, authoritarian regimes and their agents launder the proceeds of their corruption and facilitate interference operations through the European financial sector. Establishing a central European anti-money laundering authority and fully implementing existing EU-wide anti-money laundering legislation would enable more effective supervision and policing of the European financial sector. In addition, existing supervisory authorities should impose more severe fines on European entities that facilitate authoritarian regimes' malign financial activity.

7. Develop effective responses to investments by authoritarian countries and their proxies in Europe's strategic sectors

Companies, funds and individuals affiliated with authoritarian regimes have invested heavily in critical sectors of European economies, gaining these regimes access to sensitive intellectual property and infrastructure, and increasing their influence on the continent. The new EU-wide foreign investment-screening mechanism is a first step in addressing this vulnerability but should be strengthened by adding enforcement measures and enhancing the European Commission's information-gathering capabilities. Member states should also adopt screening mechanisms that follow the EU's minimum requirements and expand their own foreign investment information collection.

8. Support local and independent media

Local and independent journalism is crucial to keeping citizens involved in the political life of democracies. But its market is shrinking as funding is decreasing. In regions vulnerable to Russian disinformation, like the Western Balkans, local media often turn to Russian news outlets for content, spreading narratives damaging to Europe. European philanthropies and governments should better support local and independent media so they can endure.

9. Identify the right messengers for raising awareness about foreign interference

Efforts to explain foreign interference—and the measures countries are taking to address the challenge—should reach citizens beyond policymaking communities in capitals. Partnerships between the public sector, the private sector, and civil society should identify trusted voices in local communities to raise awareness about the foreign interference threat in a depoliticized manner and in a way that reaches the most vulnerable parts of the population.

10. Depoliticize efforts to counter foreign interference and embrace non-partisan approaches

Trust indexes show that in many countries, the public's average trust in institutions has been declining. Across the transatlantic space, the public debate on foreign interference is highly polarized. Often, facts pertaining to foreign interference are met with skepticism from the public, especially when they come from official sources. Civil society organizations are uniquely well-placed to bridge this trust gap. National governments, the EU, and philanthropic funds should better support their efforts to educate citizens and build resilience in society to this challenge.

INTRODUCTION

"It is the democratic principle that we are defending in Europe." Alcide de Gasperi (prime minister of Italy, 1945–1953).

On January 18, 2016, a video appeared on YouTube showing six armed men purporting to speak in the name of an ultra-nationalist Ukrainian battalion, threatening to conduct terrorist attacks in the Netherlands if Dutch citizens voted against an EU agreement for closer relations with Ukraine. Wearing balaclavas and military outfits, the men proceeded to burn a Dutch flag.[1] A few days later, a video from yet another YouTube channel showed a group of masked men who claimed to belong to the same battalion treading on a Dutch flag.[2] Both videos were fabricated. The independent research collective Bellingcat linked them to the Internet Research Agency, an entity based in St. Petersburg, Russia.[3] In February 2018, the U.S. Department of Justice indicted the Internet Research Agency, describing it as "a Russian organization engaged in operations to interfere with elections and political processes."[4]

Disinformation was an important tool in the Russian government's efforts to interfere in the Dutch referendum on a closer EU relationship with Ukraine. Online disinformation was supplemented by Russians, who passed themselves off as Ukrainians, working with Dutch politicians to agitate against the EU-Ukraine agreement.[5] Ultimately, 64 percent of Dutch voters rejected the measure, handing Moscow a dual victory. First, the Dutch vote prevented closer ties, albeit temporarily, between the EU and Ukraine, where Russian-supported rebels have been waging a secessionist war to destabilize the country and damage its Euro-Atlantic integration path. And second, it undermined EU cohesion as all other member states had supported the agreement.

This was not the first time the Russian government put the Netherlands in its crosshairs. For years it has waged disinformation campaigns to discredit the international investigation into the destruction of Malaysian Airlines Flight 17 in July 2014, which killed 298 people, including nearly 200 Dutch citizens.[6] The investigation concluded that Russia had supplied the missile that Russian-controlled rebels in eastern Ukraine fired on the civilian aircraft.[7] And in April 2018, the Dutch authorities caught and expelled four Russian intelligence operatives as they were attempting a cyberattack on the Organization for the Prohibition of Chemical Weapons in The Hague.[8] The failed hack was part of a Russian attempt to discredit the organization's investigation into Russian intelligence operatives' poisoning of Sergei Skripal, a former Russian intelligence officer now living in the United Kingdom, and his daughter, in the small English town of Salisbury.[9]

1 Bellingcat Investigation Team, "Behind the Dutch Terror Threat Video: The St. Petersburg "Troll Factory" Connection," Bellingcat, April 3, 2016.

2 "Fake: Azov Battalion Continues to Threaten the Netherlands," StopFake, February 1, 2016.

3 Bellingcat Investigative Team, "Behind the Dutch Terror Threat Video."

4 "Internet Research Agency Indictment," United States Department of Justice, February 16, 2018.

5 Andrew Higgins, "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote," The New York Times, February 16, 2017.

6 Ben Nimmo, "#PutinAtWar: Dismissing MH17," DFRLab, Medium, May 26, 2018.

7 "MH17: The Netherlands and Australia Hold Russia Responsible," Government of the Netherlands, May 25, 2018.

8 John Henley, "Visual Guide: How Dutch Intelligence Thwarted a Russian Hacking Operation," The Guardian, October 4, 2018.

9 Ben Nimmo, "Skripal Poisoning: If Not Russia, Then...," DFRLab, Medium, March 15, 2018.

Russian interference operations in the Netherlands over the past several years are indicative of a broader trend across the continent. The Alliance for Securing Democracy (ASD) has documented hundreds of instances of Russian interference in more than 40 democracies in the transatlantic community.[10] Using five asymmetric tools—cyberattacks, information operations, malign finance, strategic economic coercion, and political and social subversion—Russian government officials and their proxies have taken advantage of Europe's vulnerabilities to destabilize nations and fracture alliances. Russian destabilization efforts target major political events—from Brexit and Catalonia's push for independence to France's 2017 presidential election[11] and the Macedonian name-change referendum[12]—in each instance promoting Europe's most divisive voices. And it pushes fringe narratives, including distorted or fabricated stories like the false claim of a German girl's rape by migrants or the fictitious account of U.S. troops killing a Lithuanian boy, into the mainstream. The Russian government's goal is to polarize European society over these social and political issues and damage Europe's institutional fabric—the EU and NATO.

Russia is not the only authoritarian state threatening European democracy. The Chinese government is increasingly taking advantage of Europe's vulnerabilities for its own benefit, using its growing economic clout and increasing high-tech expertise to further its geopolitical objectives. Chinese state-owned companies have acquired European companies possessing sensitive technologies and intellectual property, extracted valuable know-how, and attained dominance in several strategic economic sectors.[13] The Chinese government is also attempting to reshape European discourse about China's rise through journalist exchanges and academic collaborations, ensuring that critical views of its increasingly assertive foreign policy are dampened in countries like Greece and the Czech Republic.[14] Not only has this benefitted China economically, these investments have also been used as leverage to limit the EU's ability to counter China diplomatically. For example, in Greece, the purchase of the port of Piraeus in Athens by a Chinese state-owned company has transformed an aging installation into a booming hub.[15] Shortly after the purchase, Greece blocked an EU statement against human rights violations in China.[16] Hungary, which has also benefitted from Chinese investments, has similarly stymied EU criticism of the economic giant.[17] And the Chinese government's push to create a 17+1 format with select members of the EU helps Beijing develop relationships with "friendlier" European states that could benefit China while fracturing EU unity.

> ***"Russia is not the only authoritarian state threatening European democracy. The Chinese government is increasingly taking advantage of Europe's vulnerabilities for its own benefit.***

China's leadership is developing tools to make the world more conducive to authoritarianism. The Chinese software and hardware that make up China's Great Firewall and allow the Chinese Communist Party to monitor, identify, and scrub dissent from China's online information space are now being exported—with implications for democracies. Huawei, a telecommunications equipment and consumer electronics manufacturer headed by a former officer in the Chinese military, is already embedded in the infrastructure of many European democracies. Despite warnings from several national intelligence agencies about the security risks posed

10 "Authoritarian Influence Tracker," Alliance for Securing Democracy.

11 David Salvo and Etienne Soula, "Russian Government's Fission Know-How Hard at Work in Europe," Alliance for Securing Democracy, October 31, 2017.

12 Saska Cvetkovska, "Russian Businessman Behind Unrest in Macedonia," Organized Crime and Corruption Reporting Project, July 16, 2018.

13 James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?," Council on Foreign Relations, May 13, 2019.

14 Philippe Le Corre, "China's Rise as a Geoeconomic Influencer: Four European Case Studies," Carnegie Endowment for International Peace, October 15, 2018.

15 Ilias Bellos, "Boom Awakens Memories of Piraeus's Ancient Glory," Ekathimerini, June 6, 2018.

16 Simon Denyer, "Europe Divided, China Gratified as Greece Blocks E.U. Statement over Human Rights," The Washington Post, June 19, 2017.

17 Ibid.

by Huawei,[18] several European democracies are hesitant to exclude its products from upcoming 5G networks out of reluctance to alienate a major trading partner, fear that excluding Huawei from their markets will require extensive remodeling of their telecom infrastructure, or skepticism towards the motivations behind the United States' push against the Chinese manufacturer. This has left Europe divided on a critical security challenge.

While Russia and China have conducted the most extensive interference in European democracies, other authoritarian regimes are learning from their tradecraft. For instance, Iranian information operations have begun to mimic Russian tactics.[19] Many experts now consider North Korea a cyberpower.[20] Other governments, including some within the transatlantic community, have expressed admiration for—if not adopted—authoritarian tools and tactics, either to interfere in democracies or to suppress domestic dissent.

A Blueprint for Europe to Counter Authoritarian Interference

The authoritarian threat to European democracies is not new. European nations have been on the frontlines of the authoritarian interference challenge for decades. Europe is both a thought leader and action leader in defending against this threat, but vulnerabilities across the continent nevertheless remain. Lax laws facilitate billions of dollars of corrupt money entering Europe's economies. Several European states hold an uncritical view of Chinese state-driven investments. In the information space, tech platforms, despite all the benefits their innovation has brought, still open the door for disinformation. Diffuse IT networks remain susceptible to cyberattacks, as are some election systems across Europe. As the United States has shown in recent years, no democracy, no matter how advanced, is immune from this challenge.

With technology rapidly advancing and more state actors adopting Russia's and China's playbook, Europe needs a strategic approach to countering authoritarian interference that breaks down stovepipes to address the various dimensions of the interference threat holistically. This report offers a blueprint for implementing such a response. It first analyzes measures taken to date in Europe to counter authoritarian interference, highlighting best practices and identifying ongoing vulnerabilities across the three areas on which European institutions and states have focused the most attention: disinformation, economic security, and technology. It then develops a new strategic approach for countering authoritarian interference in Europe, one that harnesses the expertise and strengths of all sectors of democratic society. It concludes with recommendations for Europe's institutions, national governments, the private sector, media organizations, and civil society.

This report builds on ASD's June 2018 *Policy Blueprint for Countering Authoritarian Interference in Democracies*, the first report of its kind to offer comprehensive whole-of-government and whole-of-society policy recommendations for policymakers, the private sector, media, and civil society.[21] Aimed primarily at an American audience, that report put the Russian operation against the 2016 U.S. presidential election in the broader context of Russian interference across the transatlantic space, analyzing the tools and techniques Moscow has honed over the years to undermine democracies. It provided an initial set of recommendations for the EU and NATO that are expanded on here. Although the present report mainly addresses a European audience, countering foreign authoritarian interference is a transatlantic challenge that will be best addressed through common and coordinated responses. Europe's best practices and missteps provide useful guidance also for the United States, Canada, and democracies outside the transatlantic community.

18 David Bond and Nic Fildes, "UK Intelligence Panel Warns on Huawei Security Flaws," Financial Times, March 28, 2019; James Vincent, "Don't Use Huawei Phones, Say Heads of FBI, CIA, and NSA," The Verge, February 14, 2018. Dušan Navrátil, "Warning," National Cyber and Information Security Agency, December 17, 2018; Gerard Taylor, "PST Believes Huawei's 5G Network Development in Norway is Problematic," Norway Today, January 16, 2019.

19 Bradley Hanlon, "Iran's Newest Info Op Shows an Evolution of Tactics," Alliance for Securing Democracy, November 13, 2018.

20 David E. Sanger, David D. Kirkpatrick, and Nicole Perlroth, "The World Once Laughed at North Korean Cyberpower. No More," The New York Times, October 15, 2017.

21 Jamie Fly, Laura Rosenberger, and David Salvo, "The ASD Policy Blueprint for Countering Authoritarian Interference in Democracies," Alliance for Securing Democracy, June 26, 2018.

THE THREAT, EXISTING RESPONSES, REMAINING VULNERABILITIES

Combating Disinformation

Of the tools used by authoritarian states to interfere in transatlantic democracies, disinformation has been Europe's primary focus. European institutions have acted to counter information operations either through dedicated initiatives or by making this fight a pillar of broader efforts to counter hybrid threats. Some national governments have proposed legislation designed to curb disinformation on social media platforms and supported media literacy and digital education programs. And European civil society, in spite of limited resources, has succeeded in shining a light on foreign authoritarian information operations targeting Europeans.

European Institutions—the EU and NATO

The numerous initiatives at the EU and NATO to combat disinformation demonstrate how seriously most member states view the challenge. These initiatives have made important strides in raising awareness about foreign disinformation, combating Russian government-sponsored disinformation, and proposing best practices for public institutions and the private sector in addressing this threat. However, they are not always coordinated to maximize their effectiveness, even if they are generally mutually reinforcing, and they sometimes lack resources or enforcement mechanisms.

One of the EU's most notable counter-disinformation initiatives is the European External Action Service's (EEAS) East StratCom Task Force. It was established to address Russian disinformation campaigns against the EU conducted in the Eastern neighborhood. The task force is effective in correcting false or misleading claims about EU policies, but its mandate is geographically limited, it remains underfunded, and its impact is difficult to assess. By the EU's own estimates, Russia spends more than a $1 billion a year on its propaganda outlets.[1] Despite doubling the budget in 2019 and establishing a Western Balkans Task Force and a Task Force South, the EU only allocates €5 million to countering disinformation.[2]

The sole public-facing element of the task forces' work is a website available in only three languages, one of which is not even an official EU language (Russian). Countering disinformation will be most effective if it comes from local actors, rather than from Brussels. The task forces' priority of strengthening the local media environment is arguably more impactful over the long-term than their counter-disinformation efforts. Support for local actors in vulnerable regions like the Western Balkans will have to be an essential component of the task forces' work to maximize their reach and impact.

The EEAS' Action Plan against Disinformation, adopted in December 2018, lists the measures the EU intended to take to counter disinformation before the May 2019 European Parliament elections and beyond.[3] The document expresses a strong resolve to act against foreign authoritarian interference, but many of the proposed initiatives, such as the establishment of a Rapid Alert System to coordinate national responses to disinformation within the EU and with other relevant actors, are still in their infancy. Its recommendations fall outside

1 Samuel Stolton, "EU Commission Takes Aim at Disinformation, Admits Funding Deficit," Euractiv, December 6, 2018, last updated January 3, 2019.

2 High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan against Disinformation," European Commission, December 5, 2018, 6.

3 High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan against Disinformation."

the scope of competences already delegated to EU institutions, leaving member states, some of which are skeptical of the disinformation challenge, tasked with implementation.

The European Commission and the High Representative of the Union for Foreign and Security Policy assessed the implementation of the Action Plan against Disinformation during the recent European Parliament elections. Notably, they attributed "continued and sustained disinformation activity" covering a range of topics to Russian sources. These disinformation campaigns attacked the EU, amplified localized polarizing content to influence public opinion, and sought to suppress voter turnout. Their report found "the measures taken as part of the Joint Action Plan against Disinformation and the dedicated Elections Package contributed to deter attacks and expose disinformation."[4]

> *"The numerous initiatives at the EU and NATO to combat disinformation demonstrate how seriously most member states view the challenge. However, they are not always coordinated to maximize their effectiveness.*

The EEAS also established the Hybrid Fusion Cell in 2016 as a hub for EU member states monitoring disinformation and cyber-related issues. However, member states may be reluctant to share classified information using this mechanism and it is unclear whether it duplicates other efforts to address disinformation across EU institutions.

Meanwhile, the European Commission has shepherded a Code of Practice on Disinformation, largely drafted and enforced by social media platforms and large advertisers. The public-private partnership forged as a result of involving the major online tech platform companies in the drafting of the code is particularly noteworthy. Moreover, the EU commissioners for security union and for digital economy and society should be commended for publicly criticizing the signatories for falling short of their commitments.[5] Yet, while the non-binding commitments in the code are promising, the lack of enforcement mechanisms and insufficient performance by the signatories should prompt the European Commission to consider more hands-on regulation of the platform companies. In its June 2019 assessment of the European Parliament election safeguards, the European Commission planned to examine the code's effectiveness after the first 12 months. Further measures, including the possibility of regulation, will be based on the findings.[6]

There is growing cooperation between the EU and NATO. The NATO Strategic Communications Center of Excellence in Riga and the European Centre of Excellence for Countering Hybrid Threats in Helsinki facilitate EU-NATO cooperation within their structures. However, this cooperation is limited by insufficient buy-in from many member states and a lack of integration into decision-making structures in both organizations. Despite skepticism from some allies, NATO has begun to take more steps to address the challenge of foreign interference, including by establishing counter-hybrid support teams to assist allies facing hybrid threats. But NATO has yet to deploy one of these teams and it remains unclear how a team would assist an ally facing a disinformation operation from a foreign adversary. This is not a hypothetical scenario. Over the past few years, allies have faced a significant increase in disinformation, particularly from official Russian media outlets, either designed to turn local populations against the alliance or to destabilize a country more broadly.

National Governments

Individual European nations have adopted their own solutions to combat disinformation, although some of the approaches create potential pitfalls.

4 High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan against Disinformation."

5 Julian King and Mariya Gabriel, "Facebook and Twitter Told Us They Would Tackle 'Fake News'. They Failed," The Guardian, February 28, 2019.

6 High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan against Disinformation."

Germany's Network Enforcement Act (or NetzDG) of 2017, which makes social media companies that inadequately moderate the content on their platforms liable to large fines, is the highest-profile piece of legislation in this area. However, the broad definition of what constitutes illegal content under the law has led social media companies to take down content that does not necessarily run afoul of the law for fear of being fined. Other European states, notably France and the United Kingdom, are also emphasizing content moderation.

> *"Self-regulation by the platforms has not effectively prevented foreign authoritarian actors from placing divisive ads on social media platforms.*

An alternative approach focused on identifying inauthentic patterns of online behavior would present fewer risks to freedom of speech. Information operations rely on deception online through a combination of fake accounts of people masquerading as concerned citizens, and of bots and computer programs that amplify content without disclosing the identity of the fake accounts. National governments should consider sanctioning these forms of malign behavior online, which would deter foreign disinformation operations while avoiding the more fraught challenge of determining which specific pieces of content promoted by foreign authoritarian actors are harmful.

On the issue of online political advertising, too few European states have passed legislation regulating political ads purchased on social media platforms. This absence of government intervention has left it to the social media companies to create their own guidelines. During the abortion referendum campaign in Ireland in 2018, foreign actors created online advertisements to influence voters, exploiting loopholes in campaign finance laws, which prohibit foreign political donations but do not regulate online ads.[7] As a result, Facebook limited the purchasing of online ads to domestic actors in Ireland, while Google banned ads related to the campaign entirely.[8]

However, self-regulation by the platforms has not effectively prevented foreign authoritarian actors from placing divisive ads on social media platforms. For example, despite Facebook launching a tool to promote online political ad transparency, there have been several reports of political ad buyers hiding their identity, a loophole foreign actors will exploit to interfere in election campaigns and spread disinformation.[9]

European governments have not simply resorted to legislation to address the disinformation challenge. Some have strategic communications teams, while in France, experts are embedded within social media companies.[10] Others have implemented anti-disinformation campaigns in schools, which rely on media and digital literacy training for students. The partnerships between government and civil society should be a model adopted throughout Europe, as trusted voices in civil society may often be better messengers than governments for pushing back against disinformation and for providing citizens the tools they need to become better consumers of information.

Civil Society

Defending against the authoritarian interference threat requires a whole-of-society approach, and civil society's role is instrumental in these efforts. Several European civil society organizations are developing novel solutions to counter disinformation. Some of the more notable initiatives include a videogame putting players in the shoes of someone seeking to spread false stories;[11] chatting in real time with citizens concerned about authenticity of articles, pictures or videos and helping them establish the

7 Emma Graham-Harrison, "Revealed: The Overseas Anti-Abortion Activists Using Facebook to Target Irish Voters," The Guardian, May 12, 2018.

8 Jim Waterson, "Google Bans Irish Abortion Referendum Adverts," The Guardian, May 9, 2018.

9 Lauren Feiner, "Political Ad Buyers are Exploiting a Facebook Loophole to Disguise Where Their Money is Coming From," CNBC, October 18, 2018.

10 "Creating a French Framework to Make Social Media Platforms More Accountable: Acting in France with a European Vision," République Française, May 2019.

11 "About the Game," Bad News.

veracity of the shared weblinks;[12] a comic-book warning Swedish children about the dangers of disinformation;[13] and journalists engaging with students to improve their ability to sort fact from fabrication.[14] Civil society and journalists have established fact-checking organizations all over Europe, while the NGO Reporters Without Borders and its partners have developed a system to "reward media outlets for providing guarantees regarding transparency, verification and correction methods."[15]

For additional information and analysis of European efforts to counter disinformation, please see Annex A.

Securing Prosperity without Sacrificing Integrity

Combatting Malign Finance

Authoritarian states take advantage of Europe's markets and financial institutions to enrich themselves and launder funds, to build relationships with local leaders, and to influence policy. The corrupt origin of these funds, and the billions of laundered euros and dollars, undermine transatlantic financial and political systems. The nature of the EU's internal market means authoritarian regimes can undermine the entire union by utilizing weaknesses in specific member states.

Large-scale money laundering scandals involving hundreds of billions of dollars, linked at least in part to Russia, have rocked Europe in recent years. The EU's financial supervisory architecture has not always been conducive to preventing illicit activity. Financial services are spread across the single market, prudential supervision is concentrated within the eurozone, and each member state has jurisdiction for its own anti-money laundering oversight. This system has made it hard for EU member states to coordinate anti-money laundering activity, and often leaves smaller ones—with their limited resources—to serve as the first line of defense. [16]

There are other vehicles for bringing dark or ill-gotten money into Europe that could be used to undermine the integrity of financial and political systems. Election finance laws that differ from country to country, for example, are a vulnerability that foreign actors can exploit. Marine Le Pen's far-right National Rally (formerly National Front) party received a loan from First Czech-Russian Bank in 2016 that was legal under French law. Italy's far-right Lega party may have been in talks with influential Russians to obtain funding for their European Parliament elections campaign, which may have been legal under Italian law. Less than half of the EU's 28 member states have a full ban on foreign donations; 11 have partial restrictions in place, but these vary dramatically from country to country.[17] Belgium, Denmark, Italy, and the Netherlands have no restrictions in place, although the Netherlands announced in January 2019 it intended to ban political donations coming from countries outside of the EU.[18] "Golden visa" and "golden passport" schemes that allow agents of foreign authoritarian regimes to buy their right to live and work legally in many EU member states also have yet to be curbed in a significant way.

Combatting malign finance from abroad will require Europe to establish a more transparent financial sector, close loopholes in election finance laws, and reduce mechanisms that allow wealthy and influential agents of authoritarian regimes to undermine European democracy legally. The EU and some of its member states have already passed legislation prescribing enhanced due diligence checks and the creation of registers listing the ultimate beneficiaries of funds or assets. These measures are necessary for rooting out dark money across Europe and should be adopted in all member states.

12 "Ako Fungujem," Checkbot.

13 Lee Roden, "Why This Swedish Comic Hero is Going to Teach Kids About Fake News," The Local, January 16, 2017.

14 Eleanor Beardsley, "A Conspiracy Video Teaches Kids A Lesson About Fake News," National Public Radio, May 3, 2018; Jason Horowitz, "In Italian Schools, Reading, Writing and Recognizing Fake News," The New York Times, October 18, 2017.

15 "More Than 100 Media Outlets and Organizations are Backing the Journalism Trust Initiative," Reporters Without Borders, February 4, 2019.

16 Joshua Kirschenbaum and Nicolas Véron, "The European Union Must Change its Supervisory Architecture to Fight Money Laundering," Brugel, February 26, 2019.

17 Kristine Berzina, "Foreign Funding Threats to the EU's 2019 Elections," Alliance for Securing Democracy, October 9, 2018.

18 "Giften Van Buiten de EU Aan Politieke Partijen Mogen Niet Meer," Rijksoverheid, January 25, 2019.

Combatting Strategic Economic Coercion

Strategic economic coercion is another growing area of concern across Europe. Russia and China are exploiting their national resources and commercial activity to gain leverage over European governments, to weaken them, to force changes in policy, and to cultivate influential proxies. Europe's energy sector is especially vulnerable to coercive investments. The legacy of the Soviet Union has made many Central and Eastern European nations' energy infrastructure deeply intertwined with Russia's, which the Russian government exploits for coercive leverage. The shutting off of gas to Ukraine in the middle of winter is a prime example of this. Abundant and cheap Russian natural gas is also fueling many of Europe's major economies. Some European countries have been keen to achieve energy independence from Russia, while others are wary of relinquishing this familiar source of energy. Energy dependence is not only a question of natural gas, it is also a concern in the nuclear sector. Four EU member states and Ukraine are dependent on Russia for nuclear fuel for their Russian-built nuclear reactors.[19]

The EU has made the following significant progress in improving common energy markets and having a single voice on energy issues.

- The European Commission in 2015 launched an Energy Union project that gives the EU a higher profile on energy issues. A newly created vice president for Energy Union has played a significant role in the EU's energy diplomacy with other countries, including Russia, Ukraine, and the United States.
- The EU has addressed technical vulnerabilities in the natural gas sector by funding infrastructure links, supporting the creation of reverse flow capacity (from west to east), and extending internal market rules to external pipelines.
- The European Commission's antitrust procedures forced Russia's Gazprom to eliminate destination clauses and change predatory pricing across Europe.

19 "Ensuring Europe's Nuclear Fuel Supply," European Commission, November 9, 2017.

Still, Russia is able to undercut European unity through large energy projects such as the Nord Stream 2 pipeline and the Paks II nuclear plant in Hungary.

> ***"Russia and China are exploiting their national resources and commercial activity to gain leverage over European governments, to weaken them, to force changes in policy, and to cultivate influential proxies.***

China has blurred the lines between the private and public sector through Chinese companies' investments in European infrastructure and technology. The fact that Chinese law compels the country's private companies to cooperate with the government upon request, and the high level of coordination sometimes exhibited by supposedly unrelated companies, suggests there is little distinction between the Chinese private and public sectors. European policymakers have put in place an EU-wide foreign direct investment (FDI) screening process in response to concern over Chinese investments.

Other European measures include:

- EU guidelines for member states to set up their own foreign investment screening mechanisms.[20]
- An EU early-warning mechanism for information sharing on ongoing FDI screening processes between member states, and with EU institutions.[21]

20 "Regulation of the European Parliament and of the Council Establishing a Framework for the Screening of Foreign Direct Investments into the Union," Council of the European Union, February 20, 2019, Art.3

21 Ibid., Art.6

- National efforts in Germany, France, the United Kingdom, and elsewhere on investment screening rules in critical areas including robotics, artificial intelligence, space, data, and semiconductors.

Nevertheless, countering malign economic influence remains difficult. The Chinese government sees Europe as the end point of its Belt and Road Initiative, a massive state-led investment plan with questionable transparency practices and clear geopolitical overtones. With China promising billions of euros, many European countries are faced with a choice between short-term pragmatic economic gain and their long-term strategic approach to emerging challenges. While the EU is still only waking up to this threat and has made attempts to shield strategic sectors from being siphoned to China, these first steps need considerable reinforcement.

Importantly, Europe is using its economic weight as a tool for countering attacks by authoritarian states. EU member states have remained united in the sanctions they have imposed on Russia for its aggressive actions in Ukraine. In particular, since March 2014, 164 people and 44 entities have had their assets frozen and travels restricted, and various import and export bans have been put in place by the EU.[22]

For additional information and analysis of Europe's efforts to secure prosperity without sacrificing integrity, see Annex B.

Securing Digital Infrastructure and Making Technology Safe for Democracy

Given the irreversible march toward digitization, foreign authoritarian actors are increasingly focusing their interference efforts on the control and disruption of IT systems. During the 2016 U.S. and 2017 French presidential elections, for example, hackers waged cyberattacks to obtain compromising information about candidates that was then leaked to the public and the media. In the case of the United States, Russian military intelligence (GRU) officers targeted IT systems pertaining to the conduct of elections, such as voter registration databases.[23] There are several examples of authoritarian regimes attacking European IT systems over the past decade, from Russian state actors targeting the German parliament and government agencies[24] as well as Estonian businesses and media outlets,[25] to Chinese government hackers penetrating the EU's Courtesy system that manages diplomatic communications between EU institutions and member states.[26]

European states and institutions have taken steps to better shield themselves from cyberattacks conducted by foreign authoritarian states. The EU established a framework within which member states can pool their capabilities, exchange best practices, and draw on each other's expertise on cybersecurity. It is also revising its critical infrastructure legislation and instituted a policy allowing it to implement countermeasures against entities that conduct cyberattacks against the EU, member states, and even third states and international organizations.[27] However, the EU's mandate to legislate on cybersecurity is limited, as member states retain jurisdiction over national IT networks. Moreover, it cannot take part in important norm-setting conversations at the United Nations.

Similarly, NATO has been putting more and more emphasis on cyber preparedness. Cyberspace is now an operational domain and cyber defense has been designated as an area for enhanced cooperation with the EU. Lastly, European states have been developing their capabilities in cyber space to match their increasingly sophisticated strategic documents. More than anything, the improved cyber expertise at the national level and better dissemination of the best practices developed by some member states lie at the cornerstone of European cybersecurity.

22 "EU Restrictive Measures in Response to the Crisis in Ukraine," Council of the European Union, March 18, 2019.

23 Special Counsel Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," United States Department of Justice, March 2019, 50-51.

24 Andrea Shalal, "Germany Detects New Cyber Attack by Russian Hacker Group -Spiegel," Reuters, November 30, 2018.

25 Damien McGuinness, "How a Cyber Attack Transformed Estonia," BBC, April 27, 2017.

26 Tim Starks and Laurens Cerulus, "Chinese Government Hackers Penetrated EU Communications Network, Cybersecurity Firm Concludes," Politico, December 19, 2018.

27 "Council Decision Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States," Council of the European Union, May 14, 2019.

However, digitization is a long-term trend, and innovations like 5G and artificial intelligence will make tomorrow's IT networks even more vulnerable than today's. As foreign authoritarian states are becoming more tech-savvy and are increasingly driving technological innovation, democracies need to critically evaluate whether and how they might allow these new technologies in their societies.

> *"As foreign authoritarian states are becoming more tech-savvy and are increasingly driving technological innovation, democracies need to critically evaluate whether and how they might allow these new technologies in their societies.*

In Europe, two particularly salient developments highlight the difficulties of navigating such a process. The General Data Protection Regulation (GDPR), the EU's flagship data protection legislation, is the world's most ambitious attempt to date to regulate the ways in which internet users' data is collected, stored, and used. Its enforcement by national data protection authorities has been hampered by lack of funding and staff. In addition, these authorities have failed to levy serious fines against violators of the GDPR. Another criticism of regulation is that the major online information platform companies have the expertise and resources to comply with regulations, whereas smaller entities that lack both have been susceptible to fines. Still, while its effectiveness is a matter of debate, the GDPR has at least started a worldwide conversation around data protection.

The inability of European countries to decisively scale back their involvement with Huawei, a company concerningly close to the Chinese security apparatus, and their reluctance to exclude it from the construction of the continent's 5G infrastructure, pave the way for new and long-lasting vulnerabilities to foreign authoritarian interference. Beyond 5G, artificial intelligence and other emerging technologies are anticipated to have a transformative effect on European economies and societies. European nations and institutions will need to reconcile themselves not only with the financial and regulatory issues this transformation will pose, but also with the potential for their misuse. Authoritarian actors are already using emerging technologies to increase surveillance on citizens, for example, and these technologies will be available for export. If Europe is to keep up the pace of technological innovation in the 21st century without harming democracy in the process, it will need to think through the long-term implications of new technologies and their rollout, and to take targeted, nuanced actions against these threats.

For additional information and analysis of Europe's efforts to secure digital infrastructure and make technology safe for democracy, see Annex C.

A NEW STRATEGIC APPROACH FOR EUROPE

Europe is at a critical juncture. European nations and institutions are struggling to counter a myriad of challenges on their borders and within their own communities. Migration, nationalist extremism, and discontent with the political status quo are among the factors dividing Europeans across the continent. Ethnic divisions in regions like the Western Balkans have yet to be fully healed and EU measures to prevent new terrorist attacks have yet to be systematically enforced. A threat to European stability is a threat to the European project of unity and prosperity.

A Europe whole, free, and at peace needs to be defended despite threats that seek to destabilize the continent, particularly Russia's invasion and occupation of Ukraine and Georgia. Yet, the overall security threat to Europe has evolved.

Europe's adversaries are less likely to use conventional military power to fight today's geopolitical battles due to their inability to challenge the transatlantic alliance militarily. They are more likely to employ asymmetric tools to compensate for their weaknesses—cyberattacks, information operations, malign financial influence, the subversion of political and social organizations, and strategic economic coercion.

Europe's institutions are primarily oriented toward conventional threats. They are also built to see threats as domestic or foreign, when increasingly the lines separating foreign and domestic actors posing security, economic, and information threats are blurred. As the past several years have demonstrated, the tactics foreign authoritarian regimes use against democracies defy these categories. Russian information operations reach Europeans through several channels, including television, radio, social media, and think tank activities, enflaming citizens' anger about the most divisive issues within their communities. But they also rely on local proxies in individual nations, who wittingly or unwittingly amplify narratives that further divide and undermine the cohesion of European society from within. Russian and Chinese investments in Europe's critical and strategic infrastructure—and their co-option of local actors across the continent—create political dependencies that slowly erode Europeans' sovereignty in domestic politics and foreign policy. Cyberattacks directly penetrate power plants, banks, and government websites, stopping business, shutting down media, and jeopardizing political processes.

These incursions into the daily lives of Europeans have increased since the Russian invasion of Crimea in 2014, and they will grow by an order of magnitude as technologies evolve and more actors adopt these tools. By using these tools to exploit existing cleavages in democratic societies and vulnerabilities in democratic governments, authoritarian regimes are trying to weaken and distract Europe and its transatlantic partners in the United States and Canada from their regional and global responsibilities, and to undermine democracy as a viable and compelling form of governance.

The success of Russia's operation against the 2016 U.S. presidential election has emboldened Putin's regime to wage more asymmetric attacks against Europe and its allies. European nations should not succumb to a false sense of security about withstanding this threat just because the recent European Parliament elections did not face an operation of similar scale. Initial assessments of disinformation in the election campaign encourage ongoing vigilance against this

"long-term challenge."[1] The European Commission and the High Representative for Foreign Affairs and Security Policy have argued that "Disinformation is an evolving threat that requires continuous research to update our policy toolbox in line with new trends and practices."[2] As more authoritarian actors adopt asymmetric tools and tactics, Europe will be confronting an increasing number of threats from various fronts.

> *"On their own, foreign policy actors at the national and European levels alone cannot address the new, multidimensional tactics used by foreign authoritarian states.*

On their own, foreign policy actors at the national and European levels alone cannot address the new, multidimensional tactics used by foreign authoritarian states. A coordinated, intergovernmental and whole-of-society response must involve all pillars of democratic society. The public sector, private companies, media, and civil society together can leverage their diverse expertise to enhance common understanding of Europe's vulnerabilities, implement already agreed measures, and forge stronger partnerships to build resilience in European society

Whole-of-Europe Approach

Europe has been on the frontlines of the authoritarian interference challenge for years. ASD's Authoritarian Interference Tracker alone catalogs over 360 incidents of Russian government-linked interference across European nations since 2000.[3] China and others are increasingly seeking to push agendas on the continent that undermine the integrity of European democracies and threaten European and transatlantic unity.

Importantly, Europe has acted to address aspects of the threat. What started as a challenge predominantly for nations closest to Russia's borders has become a problem most European governments are addressing in some capacity, while the EU and NATO have elevated the "hybrid" challenge on their respective agendas. However, vulnerabilities persist at the national level and at the level of European institutions, reflecting a lack of consensus either about the threat itself or how to defend against it. For example, EU task forces and NATO centers of excellence are undermined by a lack of resources, coordination, participation from certain member states, and integration into decision-making bodies. Some national governments are hampered by weak internal coordination, a refusal to address ongoing vulnerabilities that authoritarian regimes exploit, and, worst of all, a courtship of authoritarian actors for their own political gain.

For Europe to succeed, it needs continent-wide buy-in on tackling the authoritarian interference challenge. The EU should appoint a senior-level official to oversee and coordinate the various efforts across EU institutions and facilitate the sharing of best practices by member states. National governments should also centralize mechanisms for tracking and analyzing threats and developing policy responses. They should also address their own weaknesses—in the financial sector, in cyberspace, in election security, and in the partisanship that mires everyday politics—and lend more political support and resources to the EU institutions.

Increased national leadership would help elevate the foreign interference challenge on the pan-European agenda as well, providing more opportunities for nations to exchange lessons learned and best practices in multilateral formats and support one another in defending against the interference threat that contributes to divisions within EU and NATO. It might also provide the impetus for badly needed reforms in areas like anti-money laundering, where the absence of a central mechanism in the EU has in part enabled an environment where corrupt money

1 High Representative of the Union for Foreign Affairs and Security Policy, "Report on the Implementation of the Action Plan Against Disinformation," 1.

2 Ibid., 9.

3 "Authoritarian Interference Tracker."

can enter Europe with ease and be used to subvert the legitimate political processes of European nations. It is strategically important to keep unity on these issues between European governments and their NATO allies.

Transatlantic Responses to a Transatlantic Threat

The transatlantic partnership, led by NATO, which helped bring peace to Western democracies in the 20th century, remains essential for tackling the asymmetric security challenges of the 21st century. NATO is well-positioned to bring together heads of state and government as well as experts from the transatlantic community to forge consensus on policy measures to counter foreign interference. Yet, the allies lack consensus on whether this is an issue that NATO should prioritize as an organization, and it is unclear whether all allies have used NATO channels to share sensitive information regarding attacks on their democratic institutions and processes. Prioritizing the issue and sharing information are especially important when assessing and considering responses to cyberattacks, which have on several occasions crippled allies' critical infrastructure. NATO should also further articulate what other hybrid activity it considers a threat to the national security of allies, and, for purposes of deterrence, clarify publicly how it intends to harness alliance capabilities to defend allies from these attacks.

Transatlantic cooperation has been built into the EU's initial efforts at countering disinformation, and this model should continue as the EU expands its playbook to other areas of interference. The EEAS and European Commission designed their Rapid Alert System on disinformation to allow NATO and G7 countries to take part in detecting inauthentic behavior and alerting others of disinformation campaigns in real time. This ensures a multi-stakeholder and more global approach. Though the project has not yet moved beyond its initial stage, it represents a solid framework of cooperation for the future and should be expanded beyond disinformation to avoid the stovepipes that have historically plagued transatlantic analysis of and responses to foreign interference operations. For example, in the area of finance, greater information sharing on illicit finance and malign foreign investment would be particularly important to stem the flow of corrupt money from abroad that can infiltrate Western political systems. The EU, the United States, and Canada should also establish formal mechanisms for knowledge exchange and for coordinating crisis action on cyberattacks and other malign activities. Where possible, this cooperation should be done through the EU-NATO joint framework to reinforce cooperative efforts rather than create new mechanisms. However, bilateral cooperation between the United States and EU, particularly on the financial and economic aspects of foreign interference, should be strengthened.

> *"Transatlantic cooperation has been built into the EU's initial efforts at countering disinformation, and this model should continue as the EU expands its playbook to other areas of interference.*

Lastly, transatlantic nations are not the only democracies facing authoritarian threats. Stronger coordination with partners across the democratic world should be an integral part of a transatlantic strategy to counter foreign interference. The Chinese government's interference in Australia and New Zealand, for example, can be instructive for transatlantic nations increasingly facing a similar challenge from the Chinese party-state. Democratic countries can learn from each other and extend support to each other in countering global threats.

Raising the Costs on Authoritarian Interference

European nations and institutions must harness their combined political weight not only to identify and develop defensive measures against foreign interference, but also to raise the cost of conducting operations against their citizens. Russia, China, and other authoritarian regimes will continue to exploit Europe's vulnerabilities as long as they do not face costly repercussions for their actions. Exposure and attribution of attacks to the regimes that wage them, as well as proportionate and sustained measures in response, to include sanctions, send a clear message that brazen violations of international law and subversive interference in democracies will not be tolerated by Europe. Thus far, sanctions against Russia in response to the illegal annexation of Crimea and occupation of eastern Ukraine have been a success story for European unity and endurance—and for transatlantic unity as well. Many European nations, along with the United States and Canada, demonstrated solidarity with the United Kingdom in expelling dozens of Russian diplomats after Russian intelligence officers poisoned Sergei Skripal and his daughter Yulia in Salisbury, England.

Sanctions remain a valuable and effective tool for Europe to impose costs on authoritarian regimes, and existing sanctions on Russia should not be seen as the endpoint. For example, the United States imposed additional sanctions against individuals and entities in response to the Russian government's malign cyber activity, including for interference in the 2016 U.S. presidential election and the 2017 NotPetya cyberattack.[4] The EU and individual European nations should consider an expansion of the sanctions regime when similarly targeted. Furthermore, European nations can impose augmented fines, individual and corporate sanctions, and anti-money laundering measures to show adversaries that they are serious about stamping out money laundering and malign investments. The long-term strategic value of cleaning up Europe's financial sector cannot be overemphasized. The Russian and Chinese governments are using financial investments for politically subversive ends.

Limiting opportunities for authoritarian regimes, particularly Russia, to use energy as coercive economic leverage over European nations should also be a priority. Europe should not support energy projects like Nord Stream 2 that undermine its energy security, increase European dependence on Russian energy, and create divisions within the EU.

Imposing reputational costs should be an important component of Europe's playbook. When European leaders agreed to exclude Russia from the G8 in 2014 and issued strong statements after the Salisbury attacks, they clearly communicated that its behavior was unacceptable. The Netherlands' direct attribution of the Russian intelligence hack into the Organization for the Prevention of Chemical Weapons was valuable not only for exposing Russian intelligence methods, but also for publicly imposing reputational costs on a government covertly seeking to undermine an international investigation into the Skripal poisoning. Consistent public denunciation serves as a useful deterrent.

> *"Sanctions remain a valuable and effective tool for Europe to impose costs on authoritarian regimes.*

Speaking out against unacceptable behavior is especially important and less common in the case of China. Beijing has been willing to play off the EU's internal divisions, for instance by creating the 17+1 format that brings together select EU members from Southern, Central and Eastern Europe as well as non-EU Eastern European countries. By conducting business with only a few member states at a time, China also cultivates "friendlier" European nations that it hopes will advocate for policies advantageous to it. More significantly, companies owned by or affiliated with the Chinese Communist Party (CCP)

4 "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks," United States Department of the Treasury, March 15, 2018.

are buying European assets that reinforce its ability to infiltrate the technologies dominating the European market and its integration into Europe's critical infrastructure. The authoritarian tools of control that allow the CCP to institute a massive system of domestic repression are increasingly—and with impunity—being exported outside China's borders to the detriment of European democracy.

Adherence to democratic values has never been more important for European leaders and institutions. Respect for the rule of law, free and fair elections, and the right to privacy, among others, are pillars of European democracy that will always be more advantageous to European citizens than a descent to illiberalism.

Whole-of-Society Approach

The responsibility for protecting Europe's democracies from authoritarian interference is not one that governments can assume on their own. The role of civil society, for example, is critical to connecting political institutions with citizens, and in exposing, monitoring, and analyzing authoritarian interference. Eliminating vulnerabilities also will require the active participation of the technology companies that create and manage platforms for digital communications, as well as of the media whose role in ensuring transparency and accountability across government and society has never been more essential. Cooperation between governments, the private sector, and civil society needs to be fostered through flexible channels of cooperation and given financial and political support.

Tech and social media companies have a major responsibility in protecting society against malign influence activities. Many of the major platforms' efforts to counter foreign interference operations have at times been opaque and their policies inconsistently applied. They have not provided necessary access to data for third parties to effectively measure and evaluate their efforts to combat malicious activity, protect user data, and enforce community standards. The platforms should improve the transparency of online political ad funding and targeting, ensure that government-sponsored content and accounts are labeled properly, define and label social bots, and increase information sharing about specific threats with independent researchers, governments, and each other.

In contrast to the U.S. government's relatively hands-off approach, the EU and several European nations have taken tough stances toward the platforms to hold them accountable for their systemic failures. But they have also worked with the platforms as well. The EU's decision to include the platforms in drafting the Code of Practice on Disinformation was a valuable exercise, even if the project needs stronger verification and enforcement mechanisms to ensure that signatories thoroughly deliver and meaningfully report on their progress in the fight against disinformation. Yet, the conversation cannot end with the major platforms. More steps need to be taken to address the migration of disinformation threats to and from smaller and medium-sized social media platforms. The code of practice provides a positive jumping off point, but its voluntary, self-regulatory nature means that broader questions related to democratic norms in the tech and social media space remain unanswered.

> *"The responsibility for protecting Europe's democracies from authoritarian interference is not one that governments can assume on their own.*

Traditional media plays an essential role in providing objective, fact-based information to society. Local communities are losing trustworthy, local sources of information, and "most remaining media organizations and new internet media companies are firmly based in major metropolitan areas."[5] Governments and non-profits should encourage local, independent, and investigative journalism to keep citizens engaged in the democratic process

5 Heidi Tworek, "Responsible Reporting in an Age of Irresponsible Information," Alliance for Securing Democracy, March 23, 2018.

and less susceptible to disinformation. Furthermore, journalists should adopt norms and guidelines that ensure they exercise caution when reporting on hacked and leaked materials or quote anonymous, online social media accounts. The last few years have demonstrated how media organizations have inadvertently done the bidding of authoritarian agents by amplifying the disinformation they have seeded on social media. In the United States, a study of traditional and new media sources found that 32 of 33 major U.S. media outlets embedded an Internet Research Agency tweet in their articles between 2015 and September 2017.[6] According to one report in 2018, the U.K. press cited Russian government-linked trolls more than 100 times.[7]

Efforts to explain foreign interference—and the measures countries are taking to address the challenge—need to reach citizens beyond policymaking communities in capitals. Partnerships between the public sector, the private sector, and civil society should identify trusted voices in local communities to raise awareness about the foreign interference threat in a depoliticized manner and in a way that reaches the most vulnerable parts of the population. Governments and media can work with civil society on media literacy efforts to reduce susceptibility to disinformation. In Ukraine, for example, the global development and education organization IREX partnered with the Academy of Ukrainian Press and StopFake to bring a media literacy program called "Learn to Discern" to 15,000 people of all ages and backgrounds in Ukraine, who then shared the lessons with 90,000 others.[8] The same campaign reached 2.5 million people through billboard ads and public service announcements warning against disinformation. In Nordic countries, governments have launched several initiatives, including Finland's Media Policy Program 2019–2023, which was established to protect freedom of speech and safeguard democracy by strengthening media diversity and literacy and journalism.[9] In Lithuania, thousands of volunteer "elves" counter pro-Kremlin trolls to expose and refute falsehoods online.[10]

> *"The role of civil society in holding democratic leaders accountable is essential. Within the EU, civil society needs financial resources and greater participation from society at large in order to effectively serve this function.*

Democracy works better if everyone constructively contributes to improving it, preventing democratic backsliding and promoting fundamental values across society at large. The role of civil society in holding democratic leaders accountable is essential. Within the EU, civil society needs financial resources and greater participation from society at large in order to effectively serve this function. But support for civil society organizations and NGOs is especially important in states aspiring to join the EU, where NGOs are doing the hard work to expose, monitor, and analyze foreign interference. The EU and non-profits should increase their support for local actors in regions like the Western Balkans that are outside the union and vulnerable to asymmetric threats.

6 Josephine Lukito and Chris Wells, "Most Major Outlets Have Used Russian Tweets As Sources For Partisan Opinion: Study," Columbia Journalism Review, March 8, 2018.

7 Alex Hern, Pamela Duncan, and Ella Creamer, "Russian Trolls' Tweets Cited in More Than 100 UK News Articles," The Guardian, September 10, 2018.

8 Erin Murrock, Joy Amulya, Mehri Druckman, and Tetiana Liubyva, "Winning the War on State-Sponsored Propaganda," International Research and Exchanges Board, 2017.

9 Eva Harrie, "New Media Policy Guidelines in Finland," Nordicom, September 13, 2018.

10 Anne Sofie Schrøder, "Lithuania Has a Volunteer Army Fighting a War on the Internet," Euronews, September 28, 2017.

RECOMMENDATIONS

Europe should counter authoritarian interference by tackling its vulnerabilities in a cooperative, holistic, and society-wide manner. The section below identifies specific, actionable recommendations for the EU institutions, NATO, national governments, the private sector, the media, and civil society. These build toward the following ten principles that should be adopted across the continent.

1. Improve coordination and information sharing within and between national governments.

2. Develop collective responses to foreign interference operations in the EU, NATO, and across the Atlantic.

3. Protect the principles and institutions of democracy, remembering that our democracy is only as strong as we make it.

4. Raise the cost of interference in Europe.

5. Continue to push for transparency and accountability in the information and technology sectors.

6. Build more constructive public-private partnerships to identify and address evolving digital threats.

7. Tackle entrenched vulnerabilities in the financial sector that authoritarian actors exploit.

8. Develop effective responses to investments by authoritarian countries and their proxies in Europe's strategic sectors.

9. Support local and independent media.

10. Identify the right messengers for raising awareness about foreign interference, depoliticize efforts to counter foreign interference, and embrace non-partisan approaches.

The recommendations in this report draw on extensive analysis of recent European and national legislation and were refined through targeted roundtables in Brussels and consultations with European and U.S. experts. The recommendations aim to encourage policymakers and society at large to approach the evolving threats in a proactive, coordinated, and strategic manner. This builds on recommendations offered in ASD's 2018 Policy Blueprint for Countering Authoritarian Interference in Democracies.

EU and NATO

Improve Cohesion and Cooperation

The EU should appoint a senior-level coordinator for foreign interference

At present, different forms of authoritarian interference are tracked and addressed by many directorates general and institutions (for example, DG Home, DG Justice and Consumers, DG Digital Economy and Society, European External Action Service, European Commission, and European Parliament). Having a centralized coordinator or hub for questions of interference would allow the EU to better conceptualize the full threat, ensure that various efforts across EU institutions are synched and working toward the same policy objectives, and respond most effectively. In past European

Commissions, having a vice president in charge of crosscutting initiatives such as the Energy Union and the Digital Single Market has been helpful. A vice president for countering foreign interference would be useful for centralizing efforts and building a better common threat perception across the EU.

The EU should create mechanisms for sharing best practices across the EU and beyond

The Rapid Alert System set up among the EU institutions and member states to tackle disinformation should be expanded or serve as a model for a similar network for sharing asymmetric threat information (not limited to disinformation) between the EU institutions and all member states.

Beyond the Rapid Alert System, the EU should also work with the United States, Canada, NATO, and Five Eyes allies Australia and New Zealand through existing G7 channels and elsewhere to share practices. In addition to formal channels, the EU should work with representatives from civil society for sharing threat assessments (open source) and to exchange best practices and responses to authoritarian interference in emerging Track 1.5 formats. Regular contact between governments and experts from across the globe would allow all parties to view the asymmetric toolkit holistically and create society-wide norms to limit vulnerabilities.

The EU and NATO should maintain and deepen cooperation across existing areas

The EU-NATO joint declarations provide helpful political messaging and measures for countering various elements of the asymmetric toolkit that is used against Western democracies. Of the existing 74 proposals for EU-NATO cooperation listed in the joint declarations, those addressing hybrid threats and cybersecurity are most crucial for tackling interference. The EU and NATO should establish an information sharing joint task force to develop a common understanding of hybrid challenges and conduct a joint analysis of threats. This is a necessary baseline for building better defenses against authoritarian threats, as well as to ensure interoperability of defense capabilities to address these threats across the transatlantic community.

A joint task force would allow the EU and NATO to better see the full range of issues in the asymmetric toolkit and remove stovepipes within and between the two organizations. The joint task force should include a mechanism to share classified information between both organizations, as well as provide ways for relevant EU and NATO bodies (such as the centers of excellence and the EU StratCom task forces) to contribute information.

Continuing joint EU-NATO exercises is especially important for developing common resilience and deterrence capabilities. The EU's leadership in the 2018 hybrid crisis-management exercise and the inclusion of EU military staff and the Computer Emergency Response Team for the EU Institutions (CERT-EU) in NATO's flagship cyber exercises are good models to continue. The EU and NATO could also consider planning an exercise outside the traditional security realm; for instance, to test counter-disinformation and cyber measures to protect major elections in Europe.

EU-NATO cooperation on hybrid threats is functioning well on the practitioners' level but needs more support from political leaders in order to meet its potential. Formal consultations at senior government level, clearer expressions of political buy-in, and more frequent engagement at senior staff level (heads of the EU directorates general and NATO divisions) would help implement the measures agreed in the joint declarations.

The EU and NATO should make better use of their centers of excellence

The EU and NATO should more systematically integrate the resources, research, and activities offered by centers of excellence in their main operations and decision-making processes. The EU member states and NATO allies define the exact questions that these centers pursue, and it is incumbent on the institutions and member states to define precise and relevant questions to create tailored research that policymakers will be more likely to use.

A significant portion of the work done by centers of excellence remains confidential. Although understandable, the EU and NATO should, when possible, make their products widely available to

publicize their efforts to counter what is a society-wide threat. To the same end, both organizations should use the public dimensions offered by the European Centre of Excellence for Countering Hybrid Threats and use these resources not only for a narrow body of hybrid experts within governments but more widely. A broader uptake of best practices to counter hybrid threats will better inoculate all sectors of government against interference.

The centers of excellence have the potential not only to help government but also society more widely. When possible, they should increase their collaboration with experts in the private sector and academia. These exchanges can improve the centers' outputs, and in turn, the expertise residing in the centers can improve innovation know-how and technology across Europe. Such collaboration could contribute to the development and refinement of local expertise.

The EU and NATO should better anticipate asymmetric threats from China

While NATO and the EU are taking steps to assess and counter Russia's asymmetric threats, both organizations are giving less attention to China's economic investments, espionage, and technological rise, all of which the Chinese government uses to interfere in transatlantic democracies and threaten transatlantic security. Both organizations should develop more robust threat assessments to better understand and address these risks.

In particular, NATO, the EU, and their member states need to move quickly to create harmonized approaches to reduce the risks posed by 5G and other technologies, including facial recognition.

NATO should broaden its definition of hybrid threats

NATO's conception of hybrid threats includes much of the asymmetric toolkit but does not meaningfully address economic and financial tools of interference. It should expand its own analytic capacities in this area and draw on the EU to contribute information and analysis of economic coercion and malign finance. NATO can address foreign interference threats that are focused more on domestic vulnerabilities by elevating Article 3 on resilience as an alliance priority.[1]

NATO should further develop its public positions on hybrid threats

NATO's denunciation of hybrid attacks has the power to push allies and partners to take greater action against asymmetric threats and deter interference. It should further articulate what hybrid activity, beyond cyberattacks, it considers a threat to the national security of allies and clarify publicly how it intends to harness alliance capabilities to defend allies from these attacks.

Protect Democratic Principles and Institutions

The EU should defend democratic principles, especially the rule of law, across the union and in its neighborhood

The EU should continue to monitor the independence of the judiciary in member states and put pressure on those that are backsliding in the rule of law. The EU has a great deal of leverage in candidate countries, including in the Western Balkans, where policymakers are struggling to set up good governance systems while fending off influence attempts from Russia and increasingly China. Stronger institutions at home will be more capable of withstanding authoritarian attempts to exploit them.

The EU should implement rules to protect whistleblowers against retaliation

From the Panama Papers to the Cambridge Analytica scandal, whistleblowers have in recent years played a key role in highlighting vulnerabilities in democracies' financial and tech sectors that foreign authoritarian states can exploit. It is critical to encourage the quick passage and implementation of new EU-wide rules protecting whistleblowers. These rules should revolve around a few key principles: ensuring that companies set up safe reporting procedures, giving whistleblowers the possibility to go to public authorities when internal procedures yield inappropriate results, permitting whistleblowers

1 Nicholas Burns and Douglas Lute, "NATO at Seventy: An Alliance in Crisis," Belfer Center, February 2019.

to go to the media when there is collusion between wrongdoers and public authorities, and prohibiting any kind of retaliation against someone who reports breaches of EU law.[2]

NATO should uphold its values within the alliance and with partner countries

The North Atlantic Treaty explicitly identifies democracy, individual liberty, and the rule of law as foundational principles for its signatories.[3] NATO should encourage allies to continue to uphold these values at home and to demonstrate the advantages of democracy to partner countries. Healthy democracies are most capable of discovering and countering authoritarian interference.

Raise the Cost of Interference

The EU should continue to use sanctions and impose other financial costs to deter malign influence operations

Sanctions are among the strongest foreign policy instruments available to the EU. It has been firm and steady in its use of sanctions in response to Russia's aggressive actions in Ukraine, but it should continue to consider imposing sanctions against a wider range of individuals and entities in authoritarian regimes that use ill-gotten gains to fund malign influence operations. Other cost-raising instruments—especially visa bans, augmented fines, and anti-money laundering measures—are important tools for stamping out money laundering and malign investments.

The EU and NATO should attribute cyberattacks to specific actors in order to implement appropriate countermeasures. Attribution is essential at the EU level for the bloc to be able to use its new cyber sanctions mechanism against state officials and entities, firms, and individuals quickly and effectively.[4]

The EU should keep transatlantic unity on Russia sanctions

The EU sanctions regime should support and, where possible, act in parallel to the United States' sanctions regime to deter Russian interference in the transatlantic space. Strengthening sanctions on various sectors of the Russian economy that support the Russian government's destabilizing activity beyond its borders must be part of any credible European response.

The EU and NATO should continue to be vocal in response to asymmetric attacks

The EU and NATO should continue to push for coordinated and common responses to asymmetric attacks adopted by all member states. The NATO and EU-wide political statements after the attack against the Skripals and subsequent EU sanctions against Russian military intelligence officials show cohesion and strength. However, the fact that not all EU countries joined in expelling Russian diplomats shows the progress in coordination that the EU still needs to make.

Push for Transparency and Accountability in the Information and Technology Sectors

The EU should continue to push for greater transparency and information sharing by tech platforms

Many of the major tech platforms' efforts to counter foreign interference operations have at times been opaque and their policies inconsistently applied. There is therefore a need for European governments and institutions to provide oversight to ensure that platforms are adhering to their terms of service and held to account for systemic failures. This requires greater access to data in order for third parties to effectively measure and evaluate the companies' efforts to combat malicious activity, protect user data, and enforce community standards. And it requires greater information sharing on threats between governments and the tech companies.

2 "European Commission Welcomes Provisional Agreement to Better Protect Whistleblowers Across the EU," European Commission, March 12, 2019.

3 "The North Atlantic Treaty," North Atlantic Treaty Organization, April 4, 1949, last updated April 10, 2019.

4 "Council Decision Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States."

EU institutions should ensure that signatories to the EU Code of Practice on Disinformation fulfill their commitments

EU institutions should continue to monitor and assess social media companies' compliance with the Code of Practice on Disinformation. After assessing the actions taken by the signatories to combat disinformation, the institutions should take one of the following steps.

- If the institutions are satisfied with the code and its implementation, they should then continue to work with the signatories to improve and refine it, notably by incorporating emerging technologies and threats, providing greater clarity on terms and expectations, and adapting it to address new actors and threats. They should also encourage other companies to sign it and increase its scope.

- If the institutions are satisfied with the code's provisions but find their implementation unsatisfactory, they should, in addition to continuing to work with the signatories on improving it, introduce stricter enforcement mechanisms to incentivize better implementation of its existing provisions.

- If the institutions are broadly unsatisfied with the code, they should legislate and back up their legislation with effective enforcement mechanisms.

EU institutions should look beyond Facebook and Google to counter information operations holistically

Policymakers need to create data protection and content moderation requirements that can be applied across all online information platforms. Smaller social media platforms, such as 4chan, Reddit, and Snapchat—which are popular with young people—play important roles in information operations, often serving as launchpads for misleading content and narratives. Focusing too heavily on major social media platforms (Facebook, Google, and Twitter) will lead policymakers to miss critical nodes in the disinformation ecosystem.

Tackle Entrenched Vulnerabilities in the Financial Sector

The EU should create a central anti-money laundering authority

Abetted by local enablers, authoritarian regimes and their agents launder the proceeds of their corruption and facilitate interference operations through the European financial sector. To fix this, at a minimum, existing EU authorities such as the European Banking Authority should be granted enhanced powers over national regulators to act as a more powerful "supervisor of supervisors."[5] A more effective approach would be to centralize EU anti-money laundering supervision, either within the European Banking Authority or the European Central Bank or, ideally, a new agency. Centralizing this authority would reduce the risk of confusion and omissions in complex, cross-border cases, and allow for economies of scale that could improve the EU's overall anti-money laundering capabilities. An EU supervisor would also presumably show less of the bias that can appear at the national level, in which authorities can favor their major national banks. It is important to note that national authorities would retain a key role, as the agency should conduct supervision jointly with national competent authorities.[6]

Stronger enforcement of anti-money laundering policy, combined with stricter penalties, is possible with a centralized EU authority. The EU can also coordinate with the United States and the United Kingdom to track cross-border payments in databases created to share information. Such a system would provide an internationally sourced record to support anti-money laundering campaigns in the United States and Europe.[7] Increased transparency of the international financial system on both sides of the Atlantic can complement new and existing structures by exposing potential malign financial influences.

5 Joshua Kirschenbaum and Nicolas Véron, "A Better European Union Architecture to Fight Money Laundering," Bruegel, October 2018, 15.

6 Joshua Kirschenbaum, "Joshua Kirschenbaum's Testimony before the European Parliament Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance," Alliance for Securing Democracy, February 4, 2019.

7 Kirschenbaum and Véron, "A Better European Union Architecture to Fight Money Laundering."

Develop Effective Responses to Investments by Authoritarian Countries and their Proxies

The EU should strengthen its investment screening mechanism

Companies, funds and individuals affiliated with authoritarian regimes have invested heavily in critical sectors of European economies, thus gaining access to sensitive intellectual property and infrastructure as well as coercive leverage. It is essential that the EU is armed with legal tools to prevent adversarial foreign governments from acquiring control over critical European assets. Access to intelligence as well as better intelligence sharing between EU governments would contribute to more informed decision-making. The EU-wide foreign investment-screening mechanism, adopted in March 2019 and due to enter into force by December 2020, is a positive first step. It can be strengthened by widening its scope and enforcement measures. In particular, the European Commission should enhance its information-gathering capabilities to ensure that it can identify threats to the EU's critical interests in the strategic sectors the new investment-screening mechanism identifies. The EU may find a potential model in the United States, where the Committee on Foreign Investment in the United States adopted reforms that allow it to review foreign acquisitions even when they result in non-controlling stakes, and mandate submission of a declaration for review prior to completing a transaction in certain high-priority sectors.

Raise Societal Awareness and Resilience Against Interference

The EU should educate citizens about authoritarian interference

Efforts to explain foreign interference—and the measures countries are taking to address the challenge—should reach citizens beyond policymaking communities in Brussels and the capitals, and should present a more holistic picture of the various tools authoritarian regimes use to undermine democratic processes and institutions. The EU should support efforts to publicly expose information operations, such as the EU vs. Disinformation campaign, and other types of interference operations. It should work with national authorities, the media, and civil society to share this information in a depoliticized manner and in a way that reaches the most vulnerable parts of the population. Education should not be only about information operations but about vulnerability more broadly, including financial and cyber. The Swedish Civil Contingencies Agency's efforts to expose disinformation campaigns prior to Sweden's parliamentary elections in September 2018 are a good model for increasing societal resilience to these threats.[8]

The EU should support media literacy efforts across all member states

Many EU member states have already launched media literacy programs. Others have not. An EU-wide effort to train educators and public servants on best practices in the formulation and implementation of media literacy programs could help ensure that these are effectively integrated into school curriculums.[9] In addition, the EU should provide additional research grants aimed at assessing and evaluating the efficacy of digital and media literacy programs.

National Governments

Improve Cohesion and Cooperation

National governmens should centralize and coordinate domestic structures to tackle interference

National governments should centralize mechanisms for tracking and analyzing threats and developing policy responses. A centralized point of contact, as well as an integrated national strategy to counter interference within each government would help break down silos within and between bureaucracies to more holistically identify and counter interference.

8 "Countering Information Influence Activities: A Handbook for Communicators," Swedish Civil Contingencies Agency, March 2019.

9 All media literacy programs are not equally effective. Paul Mihaildis' work in this area shows that media literacy that only focuses on comprehension actually increases cynicism and distrust. By contrast, engaging students in creating media and journalism enhances their media literacy, helps them understand how journalism is created, and improves their writing skills.

National governments should also share models of intra-governmental cooperation with their allies and partners.

National governments should draw on and support regional, EU, and transatlantic resources to counter interference

Valuable analysis and resources for identifying and countering interference exist at the multilateral level, including at the EU, NATO, and the G7. National governments should actively draw on the information available and support initiatives like the EU's Rapid Alert System, NATO's centers of excellence or the G7's Rapid Response Mechanism through better funding, more active participation, and improved and institutionalized cooperation at all levels.

National governments should employ the principle of solidarity across the EU, especially in the energy sector, to reduce the risk of interference

Energy projects like Nord Stream 2 pit European states against each other and increase Russian state-controlled energy companies' leverage over individual states and the EU as a whole. National governments should not agree to projects that make Europe more dependent on Russian energy resources and should continue to work to diversify energy sources and improve energy security. Solidarity is a principle in the EU's Energy Union, but the values should also be extended to the EU's partner countries, especially Ukraine and in the Western Balkans.

National governments should replicate cyber best practices and implement common measures and procedures to better protect critical infrastructure

While the directive on security of network and information systems (NIS directive) has created an EU framework for cybersecurity, it is still largely up to national authorities and regulators to implement it. A particularly important aspect of this framework is the sharing of good practices. The Compendium on Cyber Security of Election Technology highlighted measures and procedures set up by various member states to better ensure that their election infrastructure is protected or at least more resilient to cyber threats. It is essential that national authorities take the spirit of the NIS directive and go beyond its parameters to share best practices pertaining to all critical infrastructure with authorities across Europe, between NATO countries, and with any partner democracy.

Securing election infrastructure and processes is especially important. National governments across Europe should implement the following best practices to make the cyber component of elections safer.

- Provision of free cyber training and support to political actors (parties, candidates and their staffs, election officials).
- Regularly scheduled penetration testing on electoral systems.
- Establishing a dedicated task force to ensure that elections run smoothly.

Protect Democratic Principles and Institutions

National governments should ban foreign funding of political parties and candidates

All European states should ban foreign donations to their political parties and candidates. However, in the case of European Parliament elections, foreign funding bans should not apply between EU member states.

Recent cases have shown that foreign authoritarian states seeking to financially interfere in European elections can do so through the purchase and editorial reorientation of a newspaper, the misappropriation of a business deal's profits, or the provision of a bank loan. National governments in Europe must reform their election finance laws in a holistic way to also protect elections from more indirect forms of financial interference.

National governments should maintain democratic values and principles, especially the rule of law and freedom of speech

Authoritarian powers take advantage of weaknesses in the governance structures of European states. Without the rule of law, for example, corruption can

go unchecked, and authoritarian states can more easily buy influence. Democracies with healthy institutions, a separation of powers, and the rule of law are best equipped to eliminate the threat of authoritarian interference. National governments should maintain democratic principles and hold their partners to the same standards.

Raise the Cost of Interference

National governments should impose greater costs on authoritarian governments interfering in European democracies

National governments should consider performing cyber operations against state actors and entities that attack or actively target critical infrastructure and wage interference operations. It is encouraging that, following the United States' lead in operationalizing offensive cyber capacity, Germany plans to achieve similar capacity by 2020.[10] These capabilities should be used in conjunction with sanctions to further raise the costs of conducting interference operations.

National governments should publicly attribute interference operations. This will make European citizens more aware of the threats their societies are facing and make it easier for national governments to conduct appropriate countermeasures against specific actors.

National governments of EU member states should deny agents of authoritarian interference access to the EU through more robust visa and citizenship procedures

The practice of granting "golden visas" or "golden passports," whereby foreign nationals receive a residency permit or citizenship in exchange for investing a certain amount of money in a given country, should be curtailed or completely reconsidered. While each country is free to determine the basis on which it chooses to admit residents and naturalize new citizens, politically exposed persons associated with authoritarian regimes should not be granted a right of residence in the EU if they are the object of sanctions by Europe or its allies.

10 Matthias Schulze and Sven Herpig, "Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them," Council on Foreign Relations, December 3, 2018.

National governments should require that agents promoting the interests of authoritarian regimes disclose their activities

An EU-wide policy similar to the Foreign Agents Registration Act in the United States that requires foreign agents working in a political or quasi-political role to publicly disclose their activities, could provide a common database of known foreign agents within the EU and allow for improved monitoring of potentially harmful activities.[11] Such a policy should be careful not to unduly restrict foreign agents' access to EU institutions. If it did, authoritarian governments could justify restricting EU officials' access to their officials and institutions.

Counter Disinformation by Pushing for Greater Transparency, Accountability, and Privacy

National governments should develop strategic communications expertise and capabilities to identify and monitor information operations carried out by foreign actors

All European democracies should designate a national authority responsible for identifying and monitoring information operations. Broader, EU- and NATO-level cooperation, particularly as it pertains to communicating specific threats to national audiences, is also essential. Ideally, more personnel, financial resources, and equipment should be made available to ensure that democracies are able to develop a robust expertise of these operations in a coordinated manner.

National governments should be careful when legislating against online information operations

While adopting new laws shows resolve to act and has laudable intentions, national governments should exercise caution when legislating in this space. Extreme care should be exercised to ensure freedom of speech principles are protected, lest transatlantic democracies inadvertently adopt the authoritarian tactics they are trying to fend off. In addition, broad and vague provisions, especially related to content moderation, can be, and have been misused by authoritarian regimes using similarly vague

11 "Foreign Agents Registration Act," United States Department of Justice.

provisions to curb free speech and target democratic activists within their own borders. EU policymakers must therefore be mindful that internet legislation has implications beyond their countries.

National governments should uphold the protection of user data

EU governments should prioritize enforcing compliance with the GDPR through fines and, if necessary, the threat of stricter regulation. Many of its provisions are designed to promote better data hygiene and to minimize the exploitation of user data for authoritarian ends. EU governments should work together to institutionalize compliance regimes for the GDPR. At the same time, the EU needs to regularly review the impact of such regulations to prevent unintended negative consequences, such as prohibitive compliance costs for small businesses.

Regardless of whether they are bound by the GDPR, national governments should determine the most appropriate mechanisms for protecting user data.

Tackle Entrenched Vulnerabilities in the Financial Sector

National governments should increase fines to counter illicit financial activities

While the proposal for a single EU anti-money laundering supervisor would address some of the issues in the longer term (see the recommendation under the EU section), national authorities within the EU and across Europe retain primary responsibility for the monitoring and enforcement of anti-money laundering rules. European governments, including Switzerland's, should increase the fines they impose on actors in the financial sector who abet authoritarian regimes' use of malign finance. When laundered amounts number in the billions, fines should number in the hundreds of millions, if not more. The current level of fines across Europe, with very few exceptions, results in an incentive structure that may inadvertently encourage the facilitation of illicit financial activity.

National governments should identify owners of companies and create public ownership registers to prevent obfuscation of financial sources

It is imperative that regulatory authorities be granted the tools they need to pierce the corporate veil where appropriate and to identify the ultimate owners of companies seeking to invest in Europe. The EU's Fourth and Fifth Anti-Money Laundering Directives, which set standards with which member states must comply, contain encouraging steps to address this vulnerability. However, as directives, they must be transposed into national legislation in order to have their intended effect. All European Economic Area countries (that is, including non-EU members to which the single market has been extended) should move swiftly to create public beneficial ownership registers in accordance with the Fifth Anti-Money Laundering directive, setting a new global standard.

Develop Effective Responses to Investments by Authoritarian Countries and their Proxies in Europe's Strategic Sectors

EU governments should adopt and utilize strong foreign investment screening mechanisms

Following the European Commission's regulation on screening of foreign direct investment in strategic sectors,[12] all member states should adopt foreign investment screening mechanisms that follow the EU's minimum requirements, most notably the avoidance of circumvention methods. These schemes should cover all the investments included in the EU regulation, from those that target "critical technologies […] including artificial intelligence, robotics, semiconductors, [and] cybersecurity" to those that affect "the freedom and plurality of the media."[13] And to prevent fragmentation of the single market, all member states should ensure that the screening mechanisms are mutually compatible.

12 "Legislative Train Schedule: A Balanced and Progressive Trade Policy to Harness Globalisation – Screening of Direct Foreign Investment in Strategic Sectors," European Parliament, May 2019.

13 "Regulation of the European Parliament and of the Council Establishing a Framework for the Screening of Foreign Direct Investments into the Union," Art. 4.

Support Local and Independent Media

Governments should support local journalism

Local journalism is crucial to keep citizens informed and involved in the political life of democracies, but the market for it is inherently small and its revenues are decreasing rapidly. Governments should ensure that this key democratic function endures. One model is the British Broadcasting Corporation's proposal to fund local news through a new charity organization called the Local Democracy Foundation.[14] Another model is Canada's initiative to provide CAD 595 million for local journalism over the next five years.[15] Tax cuts could also help support smaller media organizations with a focus on quality, and notably local, journalism.

Private Sector

Improve Transparency and Accountability in the Information and Technology Sectors

Social media companies should increase the transparency of online platforms to raise awareness and enhance resilience toward information operations

A major obstacle in spotting and countering foreign information operations is the opacity of social media companies. Companies should work to maximize transparency, while also being careful not to infringe on anonymity, which is essential for citizens and activists living under authoritarian regimes. Increased transparency should manifest in the following key ways.

Social media companies should make it easier for users to understand the nature of online platforms. When users join a social media platform, they have a right to know how it operates, what data is being collected, and how/why certain content is being served to them. Informed consent is key to educating users and will help build resilience against potential manipulation. Companies should also provide more information on the origin of content and why it is being shown to users, as this context is key to evaluating information. This should include information on why certain ads are being presented, and what demographics those ads are targeting.

Social media companies should work to define and label bots. While many accounts employ a mixture of human activity and automation, platforms should inform users when an account is primarily automated. This information may be helpful for evaluating information, and users have a right to know whether they are interacting with a real person or not.

Social media companies should ensure that government-funded content and accounts are accurately labeled as such. This context is important for users who are attempting to assess validity or bias in content. While YouTube attaches disclaimers to videos produced by government-funded entities, platforms should establish clear disclosure requirements for all government-funded news publishers as well as for their various online offshoots.

Social media companies should improve the transparency of political ad funding. Clearly labeling political advertisements with the names of funders, and providing users with access to information on funders, will help build resilience against manipulation. Facebook has already implemented these policies in many countries; however, these practices need to be adopted more broadly and should apply to issue-based as well as political ads. Additionally, companies should verify that advertisers are accurately representing themselves and are not using an inauthentic persona or false identity to purchase ads.

Social media companies should increase information sharing with independent researchers, governments, and the public regarding removed accounts. While companies have made some progress in sharing details of the inauthentic networks removed from their platforms, more transparency is necessary. Companies should share archived versions of removed networks with researchers (with personal data removed) to facilitate better understanding of the tactics and targeting of information operations.

14 Jim Waterson, "BBC Plans Charity to Fund Local News Reporting in Britain," The Guardian, March 19, 2019.

15 Daniel Leblanc, "Media Sector Gets $595-Million Package in Ottawa's Fiscal Update," The Globe and Mail, November 21, 2018.

Companies should also take steps to contact and inform users who have interacted with accounts or groups connected to inauthentic networks. Finally, companies should commit to uniform data standards when they release information to researchers, governments, and the public. Currently, they release data in a variety of different formats, making it difficult to process and analyze.

Social media companies should focus primarily on identifying bad actors and inauthentic behavior

Social media companies play a critical role in identifying inauthentic behavior that bad actors use to manipulate people through divisive content on online platforms. Unlike terrorist propaganda or hate speech, content posted by foreign manipulators often does not violate internet companies' terms of service or community standards. Content moderation alone will therefore not effectively combat malign foreign interference on social media. Instead, social media companies should commit to developing technologies and tools to identify bad actors and the inauthentic behavior they use to manipulate and deceive people online, and tweak their algorithms to limit the virality of content spread by bad actors. Internet companies should also engage national authorities and other key stakeholders when developing and implementing their procedures for suspending accounts, consistent with terms of service, to improve public-private dialogue around the threat of foreign interference.

Social media companies should create industry standards for content moderation

As explained above, content moderation should only play a supporting role in a framework revolving around identifying inauthentic behavior. In addition, content moderation should be conducted in a consistent and predictable manner. Internet companies should therefore adopt industry-wide standards to harmonize content-moderation systems and enforce their terms of service comprehensively, consistently, and in a timely manner. This process should involve independent, third-party oversight to ensure that companies are removing illegal content without inadvertently affecting protected speech.

Social media companies should improve cross-platform and intra-platform information sharing to enhance responsiveness to inauthentic behavior online

Social media companies should institutionalize information-sharing bodies across platforms to facilitate communication about potential threats and inauthentic activities, and to coordinate efforts to quickly respond to cross-platform information operations.

Effective action to counter cross-platform operations will require cooperation from stakeholders across the online information space. The EU has already brought some of the social media companies together in drafting its Code of Practice on Disinformation, and a similar model should be adopted for institutionalizing information sharing. The companies should involve EU institutions and national governments in their cross-platform initiatives to maintain open channels of communication and information sharing.

Social media companies should adhere to commitments under the EU Code of Practice on Disinformation

Social media companies should work to adhere to their commitments as laid out in the EU Code of Practice on Disinformation. They should also provide policymakers with appropriate information and updates to facilitate monitoring and implementation of the code, and they should work with EU institutions to ensure that the code continues to be updated and improved.

Online advertisers should leverage ad spending to encourage a healthy information ecosystem

By demanding greater control over where ads appear online, advertisers should ensure that they are not financially supporting sites or accounts that promote divisive, false, or misleading content. This will help reduce the prevalence of disinformation and will contribute to a healthier information ecosystem. Organizations like the International Fact-Checking Network and NewsGuard already provide services to help advertisers identify sites that produce misleading and inaccurate content, and, conversely, those that follow basic journalistic standards. Advertisers

can and should go a step further by prioritizing ad placement on sites or platforms that support independent, principled, and local journalism.

Advertisers have a self-interest in ensuring that their purchased content generates engagements with real users, and should therefore play a leading role in demanding transparency and integrity from social media companies. Left unchecked, bots, fake accounts, and inauthentic networks contribute to ad fraud by misrepresenting the real impressions made by an ad purchased on a platform. Advertisers have the financial leverage necessary to compel online platforms to remove these harmful actors and to combat inauthentic behavior. This, in turn, will help degrade the fake ecosystem that foreign manipulators use to boost the visibility of their content or to create "manufactured consensus."

Build Constructive Public-Private Partnerships to Identify and Address Evolving Digital Threats

Technology companies should factor the potential disruption of future technologies on democracy in their design decisions

New advances in technology, notably in the field of artificial intelligence, are bound to disrupt democracies' already fast-evolving online information spaces. For instance, the anticipated sophistication of deep fakes, as well as synthetic written and audio content, will make false content more difficult to detect and potentially more persuasive than manipulated images. Companies need to think critically about how malign actors could manipulate these technologies and make that analysis integral to the design of new features and products.

Technology companies should establish partnerships to navigate potential negative implications of future technologies

Companies should work with European government agencies, in particular the national security community, to identify potential vulnerabilities created by technological innovations. One step would be to hire technical and intelligence experts to hypothesize and test potential vulnerabilities with new products before they are publicly released.

Strong public-private partnerships should ensure that companies communicate emerging threats on their platforms to decision-makers (and vice versa).

Reduce Malign Investment and Money Laundering Activities across Europe

The financial sector and other businesses should enhance the ethical role of intermediaries

Authoritarian regimes and their proxies target various sectors of the economy. The private businesses involved all need to take a greater role in eliminating their vulnerabilities to malign influence. In the case of anti-money laundering, while regulation and streamlining of supervisory frameworks can help reduce democracies' vulnerability to authoritarian malign finance, the financial sector is ultimately responsible for enforcing any new measure in good faith. Actors in sectors ranging from real estate to art and commodities trading should ensure that ill-acquired gains are kept out of democratic economies and societies. They should play their part in ensuring that due diligence checks are carried out properly and closer attention is paid to politically exposed persons' affiliation with authoritarian regimes.

Media Organizations

Improve Transparency of Media Governance and Ownership

Media organizations and journalists should enhance their transparency and rebuild trust with the public

Media and journalists play an important role in upholding trust and factual information about democratic institutions and processes. This is especially significant at a moment when freedom of the press is increasingly under attack. While part of the trend of declining trust is due to malign information operations and thus outside of their control, media companies can still take steps, particularly in the realm of transparency, to rebuild trust with their audience. In particular, media outlets should take the following steps.

- Make their governance more transparent. Some third-party outfits such as NewsGuard have begun to rate the reliability of media outlets based on criteria such as the availability of information on ownership and financing, or whether potential conflicts of interest are made public. Media companies should take such criteria into account and adhere to the highest identified standards of corporate transparency.

- (Re)affirm their commitment to strong ethical principles. All media outlets should develop and make public an editorial code of conduct explaining their policies on attribution, use of anonymous sources, and correction, while avoiding the spread of unverified, hacked, and leaked information that could be in service of an authoritarian interference operation. They should also support initiatives that aim to create ethical standards for journalism without harming freedom of expression.

- Work to educate the public on journalistic norms and processes. Few people outside of the media industry know the process of a newsroom. By creating and disseminating materials that explain how professional journalism works, media companies would dispel some of misunderstandings that surround their daily operation.

Raise Society-wide Awareness about Foreign Interference

Media organizations and journalists should use great caution when reporting on leaked material

Stealing and leaking compromising material is a tried and true method of foreign authoritarian interference. To avoid being used as unwitting channels of information intended to damage democracy and serve authoritarian interests, media organizations should take the following steps.

- Distinguish between reporting on hacking operations and reporting on the content of the leaked information. During the 2017 presidential election campaign in France, French journalists covered the story of the hack of Emmanuel Macron's campaign e-mails without reporting on the content of the data. By contrast, during the 2016 U.S. presidential election campaign in the United States, U.S. media's reporting on the hacking and data dump of Hillary Clinton campaign e-mail accounts injected a foreign state's political agenda into an already hyper-politicized environment.

- Verify any information before it is published and contextualize in reporting how it was obtained, and provide information on the motivations behind the hack.

Media organizations and journalists should use all available presentation tools to make a story accessible to the wider public

Many stories that are currently reported require a significant amount of prior knowledge to understand. Media companies should more systematically use all the communications tools available to them, especially online. They should do the following.

- Include more visuals, notably infographics, that catch the eye and can easily be shared and convey information imaginatively on social media.

- Include explainers, including links referring to past events, tied to a news story. For instance, The Guardian and The Financial Times now incorporate options to "read more" about a given topic within their news stories.

Media organizations should support investigative journalism

Investigative journalism is expensive and time-consuming, yet its watchdog function is critical for democracy. Newer, and often smaller, independent media outlets have successfully used crowdfunding and social media to finance and create higher user engagement around investigative journalism. In addition, the success of well-researched TV shows such as Last Week Tonight in the United States, or Envoyé Spécial in France shows that there is a market for this kind of reporting. Media organizations should ensure to the best of their abilities that those who conduct this line of work receive adequate financial and, where needed, legal support.

Improve Cooperation and Coordination

Media organizations should support fact-checking as part of the solution to counter disinformation

Although media organizations conduct fact-checking during their reporting, the number of organizations specifically dedicated to it has increased substantially over the last few years. Media organizations should draw on these new resources by developing partnerships with these fact-checking organizations such as Correktiv in Germany or Newtral and El Objetivo in Spain. The additional resources provided by fact-checking organizations are especially valuable during time-limited initiatives around specific events like elections, or to pool national fact-checking resources, like Sweden's factist.se during Sweden's 2018 general elections.

Media organizations should explore new business models

Media organizations should undertake in-depth examinations of, as well as experiment with, new business models for journalism. Publications will have to find alternatives to the conventional business models for journalism based on a combination of subscription and ads. No one has a definitive solution and media organizations may find that different business models work for different types of news or organizations. For example, new or struggling media organizations might try ad-free, subscription-financed publications that rely on a tightly-knit online community to conduct longer term projects without immediate pressure to turn a profit. News organizations such as Mediapart, eldiario.es, and De Correspondent have used this crowdfunding model based on no ads and increased user support to great effect.

Civil Society

Improve cooperation and Coordination with the EU and National Governments

Civil society should actively engage governments and EU institutions

Civil society organizations should engage in regular dialogue with policymakers, and where appropriate, more actively engage them in their flagship activities. In countries where democratic principles are challenged, civil society can pressure policymakers to uphold democratic norms, including by using EU actors—from officials in the EU institutions to members of the European Parliament—as conduits to national officials who may be hostile to domestic civil society actors. Where democratic principles are not under threat, policymakers' engagement with NGOs can enhance the impact of civil society's work and also connect policymakers with the wider public. This scenario allows NGOs to set the agenda with policymakers.

Push for Greater Transparency and Accountability Online

Civil society should act as a watchdog for foreign interference on tech platforms

European democracies are home to hundreds of millions of social media users who engage in public debate in dozens of languages. Using its knowledge of local languages and contexts, civil society should help the companies operating these platforms spot malign behavior so the companies can take action. In addition, civil society should use its connection with the wider public to raise awareness about social media companies' enforcement of their terms of service and hold them accountable when they fail to enforce these comprehensively, consistently, and in a timely manner.

Civil society should pressure advertisers to stop advertising on platforms or websites known to distribute harmful content

Civil society can play a key role in ensuring that advertisers do not financially support actors promoting misleading or inaccurate content. By

identifying and calling out major advertisers that continue to advertise on such sites and pages, civil society organizations can help pressure advertisers and social media companies to contribute to a healthier online information ecosystem.

Raise Awareness about Authoritarian Interference

Civil society should extend the dialogue about foreign interference to new locations and audiences

While the EU institutions and national governments play an important role in explaining foreign interference to the public, civil society can build on these official efforts and bring that conversation closer to even more people.

Civil society should reach out to all generations with a focus on those most vulnerable to spreading disinformation. Many of the anti-disinformation initiatives in Europe center around schools and teaching young people to identify false content online. While these efforts should be maintained, there is also a need to engage older generations, which have been proven to be more likely to share false stories.[16] The media literacy campaign conducted by IREX in Ukraine is a good example of how to engage each generation in a way best suited to its tech savviness and media consumption habits.

Civil society organizations tend to be concentrated in large European countries and in capital cities. They should make more efforts to reach out to citizens outside of capitals. One way to do so is by building partnerships with local authorities, and by holding talks in smaller cities. For instance, in the United States, ASD experts have reached out to audiences outside Washington, D.C., most recently in Florida and Texas. These efforts should be replicated by think tanks and other organizations, and expanded to European non-capital cities.

Civil society should develop creative and innovative tools to empower and engage the public on interference issues

NGOs and other civil society groups often have the flexibility and operational freedom to adopt more novel and creative approaches than bureaucratic structures. Efforts such as BadNews' disinformation videogame are appealing ways to raise awareness about critical issues among the general public.

Civil society should engage with social media influencers across various themes to counter information operations and raise awareness

Countries on both sides of the Atlantic have a deep pool of young and talented content creators who have blossomed thanks to social media and are interacting with their audience in new and engaging ways. This group has a direct stake in the future of social media and would be among the hardest hit by any draconian legislation in this space. Institutions, governments and non-profits working to counter foreign authoritarian interference, particularly information operations, should reach out to these influencers and work with them to raise awareness about this issue with a wider audience.

Make Foreign Interference a Citizen Concern

Civil society should help lead the conversation on foreign interference

Trust indexes show that informed public's average trust in institutions has been declining in several countries.[17] As is the case in the United States, many European states now have a very polarized public debate where facts pertaining to foreign interference are met with skepticism from the public, especially when they come from official sources. But authoritarian interference in democracies affects everyone and the spread of false narratives, corruption, and loss of agency that follows in the footsteps of disinformation, malign finance, and other asymmetric tools should be made visible and clear to the publics of democracies, irrespective of partisan preferences. With large parts of the media

16 James Devitt and B. Rose Kelly, "Fake News Shared by Very Few, But Those Over 65 More Likely to Pass on Such Stories, New Study Finds," New York University and Woodrow Wilson School, January 7, 2019.

17 "2018 Edelman Trust Barometer: The Employer Advantage," Edelman, 2018.

also affected by general distrust, civil society should step in to help citizens gain access to reliable data and into healthy public debate.

Crowdsource the defense of democracy

In countries where the public has been made aware of the threat of authoritarian interference, many citizens have already taken it upon themselves to do something to fight back. For instance, in Lithuania, a small group of volunteers has come together to identify, report, and debunk the divisive content spread online by Russian trolls. The efforts of these "elves" have since inspired many more to follow their example. NGOs, think tanks, and other civil society participants should aim to encourage this kind of grassroots response. Calls to the public by innovative researchers like those at Bellingcat show the tremendous and untapped potential of the public's collective intelligence, online and offline.

Citizens across Europe are capable of protecting their democracies by supporting the work of governmental and non-governmental campaigns, advocating for policy change at the national and international level, and fighting for the respect of European values. Democracy can be defended by those who live under it and European citizens have the opportunity, and the responsibility, to hold elected officials, institutions, and the private sector accountable.

ANNEX A. EUROPEAN EFFORTS TO COUNTER DISINFORMATION

European Institutions

The EEAS StratCom Task Forces

Alarmed by Russia's disinformation-heavy interference campaign in Ukraine following its illegal annexation of Crimea, the EU established the East StratCom Task Force in September 2015. The task force has been observing and countering Russia's disinformation activities since then, notably by launching the EU vs. Disinfo[1] website to expose false narratives to the wider public. The European External Action Service (EEAS) later set up two additional task forces to counter disinformation in other areas of the EU's neighborhood: the Western Balkans Task Force and Task Force South. The EU more than doubled the budget it allocates to countering disinformation to €5 million in 2019.[2] While the East StratCom Task Force has taken the lead in tackling disinformation and is slated for the biggest increase in personnel and funds, the other two will also see an increased role.[3] In particular, all EEAS strategic communication teams are acquiring more media monitoring and data-analysis capacity.

However, these teams still need far more resources and a larger mandate to be an effective rampart against foreign authoritarian disinformation. By the EU's estimates, Russia spends more than a $1 billion a year on its propaganda outlets.[4] This affords Russian outlets the opportunity to have offices and personnel in many EU member states. As part of the EEAS, the StratCom task forces should focus on information operations run from outside the EU, but this does not mean that EU citizens should not be made aware of their work. At present, their sole public-facing element is a website available in only three languages, one of which is not even an official EU language (Russian).

These limitations are notable in vulnerable regions like the Western Balkans. Pro-EU messaging should remain a component of the task forces' work, but its reach will remain limited without sufficient messaging in local languages. The task forces prioritize the strengthening of the local media environment. This is arguably a more impactful objective than their counter-disinformation operations. Countering disinformation will be most effective if it comes from local actors, rather than from Brussels. The task forces' efforts to cultivate local expertise in those countries and assist independent local media and civil society actors committed to strengthening local journalism will pay long-term dividends.

The Code of Practice on Disinformation

While the EEAS focuses on disinformation targeting the EU's neighborhood, the European Commission has worked to tackle disinformation spread online within member states. In November 2017, it set up a high-level group of experts to brainstorm policies to "counter fake news and disinformation spread online."[5] In March 2018, the group released its conclusions. Crucially, it advocated for "a self-regulatory approach," at least "for the short to medium term."[6] Acting on that recommendation,

1 "About," EU vs. Disinfo.

2 High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan against Disinformation," 6.

3 Ibid., 5.

4 Stolton, "EU Commission Takes Aim at Disinformation, Admits Funding Deficit."

5 "Next Steps Against Fake News: Commission Sets Up High-Level Expert Group and Launches Public Consultation," European Commission, November 13, 2017.

6 "Final Report of the High Level Expert Group on Fake News and Online Disinformation," European Commission, March 12, 2018, 6.

in September 2018, the EU and private-sector stakeholders published a Code of Practice on Disinformation.[7]

The initiative's greatest strength was to bring private-sector stakeholders on board voluntarily, including the major online platforms and tech companies (Facebook, Google, Twitter, Mozilla, and Microsoft), as well as trade associations representing the advertising sectors. The signatories all pledged to take rapid action to better defend against foreign digital disinformation ahead of the May 2019 European Parliament elections, with a focus on four issues: increasing ad transparency, regulating bots, eliminating fraudulent or misleading accounts, and increasing cooperation between states and researchers in identifying disinformation campaigns.

> "*For now, the EU institutions have abstained from adding enforcement mechanisms to the Code of Practice on Disinformation or creating their own rules via legislation.*

Starting in January 2019, the European Commission and signatories to the code have each published monthly assessment reports on its implementation.[8] Although these reports show slow but real progress, notably concerning ad transparency,[9] the EU commissioners for security union and for digital economy and society have publicly criticized the signatories for falling short of their commitments.[10] They bemoan that none of the reports includes data assessing the effectiveness of measures taken by the signatories to monitor ad placements. They also highlight the failure of social media companies to work with fact-checkers in all of the EU's official languages and with independent researchers.

A broader concern relates to the way in which social media companies report on their implementation of the code of practice. The data they provide are given without any context. For example, when a company reports having acted upon hundreds or thousands of incidents on its platform, there is no way for officials or researchers to investigate these incidents themselves. But the main weakness of the code of practice is that it is not legally binding. Although the signatories commit themselves to adhering to certain "relevant commitments," there is no mechanism to enforce the pledges or sanction non-performance. For now, the EU institutions have abstained from adding enforcement mechanisms to the code or creating their own rules via legislation. But it bears recalling that the high-level group of experts who recommended the creation of the code only saw it as a "short to medium term" solution.

The Action Plan against Disinformation

In December 2018, the EEAS issued an Action Plan against Disinformation. It is the EU's first public document naming Russia as one of the "external actors" using disinformation.[11] The action plan is meant to bring together the various strands of the EU's anti-disinformation efforts and contains recommendations around four priorities.[12]

- Increasing resources and capabilities for existing bodies.
- Increasing cooperation and information sharing between all member states.
- Ensuring that the code of practice is implemented effectively.
- Building resilience on a societal level.

7 "Code of Practice on Disinformation," European Commission, September 26, 2018.

8 "First Results of the EU Code of Practice Against Disinformation," European Commission, January 29, 2018.

9 "Third Monthly Intermediate Results of the EU Code of Practice Against Disinformation," European Commission, April 23, 2019.

10 King and Gabriel, "Facebook and Twitter Told Us They Would Tackle 'Fake News'. They Failed."

11 High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan against Disinformation," 4.

12 Ibid., 5.

With these priorities in mind, member states established a Rapid Alert System (RAS) to coordinate national responses to disinformation within the EU and with other relevant actors, such as NATO and the G7, which has established its own Rapid Response Mechanism. Launched in March 2019, the RAS is still a work in progress.[13] Most member states have designated points of contact for the system but it cannot deliver real-time data or alerts yet. The action plan envisages an active role for national authorities and civil societies. Some member states have already launched pilot versions of the "targeted campaigns for the public" that were also envisioned in the action plan and are meant to build societal resilience, deepen cooperation with fact-checkers and researchers, and reinforce support for independent media.[14]

The action plan has the potential to make national and EU institutional efforts to counter disinformation more effective and better coordinated. Now the EU and its member states must work to execute the steps the plan lays out. This means ensuring that the RAS lives up to its name by expeditiously coordinating responses to disinformation, giving the StratCom task forces the means and mandate to effectively detect and monitor disinformation around the EU and in its neighborhoods, implementing the objectives of the code of practice, and supporting member states and civil society in their efforts to counter disinformation campaigns.

The EU Hybrid Fusion Cell

In addition to its dedicated anti-disinformation efforts, the EEAS created the EU Hybrid Fusion Cell within its EU Intelligence and Situation Centre in April 2016. The Hybrid Fusion Cell is tasked with monitoring cyberattacks and foreign attempts "to undermine public trust in government institutions or exploit social vulnerabilities."[15] Countering disinformation is thus one part of its broader mandate. In this context, the cell and the East StratCom Task Force coordinate work on Russian information operations and communicate with EU institutions and member states. The cell has already produced over 100 assessment reports and briefings for the EU institutions and member states.[16]

> ***"The action plan has the potential to make national and EU institutional efforts to counter disinformation more effective and better coordinated.***

Despite the Hybrid Fusion Cell's mandate, the EU has a limited role in regulating cybersecurity throughout Europe. The EU's Cybersecurity Act reinforces the mandate of the EU Agency for Cybersecurity and boosts the cybersecurity of online services and consumer devices, but most other cybersecurity matters still firmly remain a national competence.[17] The EU's institutional expertise in cyber-related issues is limited, and it relies primarily on seconded national experts who return to their respective capitals after a few months or years in Brussels. The EU has thus struggled to build enduring expertise and institutional memory in these fields.

The Hybrid Fusion Cell also fosters intra-EU institutional cooperation by providing quarterly reports to an inter-service group for countering hybrid threats consisting of representatives from the EEAS and the European Commission.[18] In turn, the inter-service group contributes to increased communication between EU institutions, leading

13 "Factsheet: Rapid Alert System," European Union External Action Service, March 15, 2019.

14 High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan against Disinformation," 11.

15 "FAQ: Joint Framework on Countering Hybrid Threats," European Commission, April 6, 2016.

16 "Joint Report to the European Parliament, the European Council, and the Council on the Implementation of the Joint Framework on Countering Hybrid Threats from July 2017 to June 2018," European Commission, June 13, 2018, 2.

17 "State of the Union 2017 - Cybersecurity: Commission Scales Up EU's Response to Cyber-Attacks," European Commission, September 19, 2017.

18 High Representative of the Union for Foreign Affairs and Security Policy, "Joint Staff Working Document: EU Operational Protocol for Countering Hybrid Threats – 'EU Playbook,'" European Commission, July 5, 2016, 4-5.

to new opportunities for joint action and to more effective coordination of overall EU institutional efforts.

Efforts at NATO

NATO is increasingly a target of disinformation from Russian outlets and it is taking this seriously. In addition to monitoring and debunking disinformation, the alliance is creating tools for countering information operations in the context of broader hybrid threats. Still, NATO's ambition in countering disinformation is relatively modest and the issue is largely portrayed as a regional rather than alliance-wide concern.

At the Wales Summit in 2014, shortly after Russia's illegal annexation of Crimea, NATO member states pledged to "[enhance] strategic communications, [develop] exercise scenarios in light of hybrid threats, and [strengthen] coordination between NATO and other organisations."[19] At the time of the Summit, NATO had recently accredited a Center of Excellence on Strategic Communications in Riga, which, together with the Public Diplomacy Division and other parts of NATO, develops analysis to counter Russian and other disinformation aimed at the alliance.[20]

Since its enhanced forward presence deployed in the Baltic states and Poland in June 2017, NATO has been targeted by a barrage of disinformation aimed at turning public opinion in allied countries against it and dissuading the public in neutral countries from wanting to join the alliance. Official Russian media outlets have spread anti-NATO stories, including the false accusation that German troops committed rape in Lithuania,[21] the portrayal of the Canadian contingent in Latvia as a cross-dressing "Gay Battlegroup,"[22] and the fabricated story of a U.S. Army vehicle hitting a boy on a bicycle in Lithuania.[23]

In Sweden and Finland, two EU countries that are NATO partners but not members, Russia has conducted sustained disinformation operations against the North Atlantic alliance. The most recent unclassified yearly report from Swedish intelligence explains that keeping Sweden out of NATO is a "Russian strategic objective."[24] NATO was among the top three subjects of disinformation on a short-lived Swedish Sputnik outlet.[25] In 2015, Russian media circulated fake letters purportedly signed by Swedish officials, including the minister of defense, on the subject of NATO and Ukraine.[26] The letters were intended to spread disinformation and impact public opinion on the conflict in Ukraine. Finland is also the target of Russia's information operations. There, false stories and information campaigns have coincided with military aggression from Russia, such as airspace violations.[27]

> ***"NATO's ambition in countering disinformation is relatively modest and the issue is largely portrayed as a regional rather than alliance-wide concern.***

At the Brussels Summit in July 2018, NATO agreed to establish counter-hybrid support teams. When member states need support, they may request tailored targeted assistance in a variety of areas, including countering disinformation.[28] However, NATO has not yet deployed a counter-hybrid

19 Heads of State and Government, "Wales Summit Declaration," North Atlantic Treaty Organization, September 5, 2014.

20 "NATO – Russia: Setting the Record Straight," North Atlantic Treaty Organization, February 1, 2019.

21 Teri Schultz, "Why the 'Fake Rape' Story Against German NATO Forces Fell Flat in Lithuania," Deutsche Welle, February 23, 2017.

22 Chris Brown, "Anti-Canada Propaganda Greets Troops in Latvia," CBC, June 16, 2017.

23 Andrius Sytas, "Lithuania Sees Fake News Attempt to Discredit NATO Exercises," Reuters, June 13, 2018.

24 "Arsbok 2018," Säkerhetspolisen, 2018, 30.

25 Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence Through Public Diplomacy and Active Measures: the Swedish Case," Journal of Strategic Studies, 2017.

26 "Russia Spreading Fake News and Forged Docs in Sweden: Report," The Local, January 7, 2017.

27 Reid Standish, "Why Is Finland Able to Fend Off Putin's Information War?," Foreign Policy, March 1, 2017.

28 "Brussels Summit Key Decisions: 11-12 July 2018," North Atlantic Treaty Organization, November 2018.

support team and the precise modality of what kind of experts would form such teams is still under consideration.[29]

While the Strategic Communications Centre of Excellence in Riga is not part of the NATO command structure, it contributes to the alliance's efforts to tackle Russia's disinformation campaigns and conducts research and training, which in turn can complement NATO policies and operations. For instance, in late 2018 and early 2019, researchers from the center tested the vulnerability of NATO soldiers to social media manipulation by luring them to fake accounts and groups.[30] The center also supports a variety of exercises that contribute to NATO-EU cooperation on crisis management and capability development.

Lastly, since 2016, NATO's Allied Command Transformation in Norfolk, Virginia, in the United States has taken a larger role in the fight against disinformation, in particular to "support coherent and successful strategic communication" by developing methods and tools to help detect and identify disinformation and the signs of potential hybrid activities early.[31]

NATO-EU Cooperation

Reflecting the allies' decisions at the Wales and Warsaw summits, NATO and the EU have increased cooperation on hybrid challenges, including disinformation. Formal cooperation on hybrid threats started in 2016 with the signing of a joint declaration and was expanded in 2018 to further areas.[32] According to a progress report on the first two years of cooperation, the two organizations had "exchanges at the technical level" on strategic communications as well as "frequent engagement between EU and NATO spokespersons, strategic communications counterparts and the EU Strategic Communications Task Forces, and the NATO Strategic Communications Centre of Excellence in Riga."[33]

In 2017 and 2018, the EU also conducted counter-hybrid crisis management exercises that ran in parallel with NATO staff command post exercises. The objectives of the exercises were to recognize a hybrid threat more quickly, counter a cyberattack, and improve crisis response and strategic communication.[34] Continuing these exercises will contribute to better coordination and interoperability of participating countries' capabilities to address asymmetric threats.

> ***"EU-NATO cooperation on countering disinformation is visible in the NATO and EU centers of excellence.***

EU-NATO cooperation on countering disinformation is visible in the NATO and EU centers of excellence. Sweden and Finland, EU members but not NATO allies, contribute to the Riga center's activities and lend their expertise to its research.[35] The European Center of Excellence for Countering Hybrid Threats opened in April 2017 in Helsinki as an initiative to assist the EU, NATO, and their member states. States need to join in their individual capacity, and the number of participating countries has increased from 9 to 21 since the center's creation.[36] The Helsinki center, which "maintains close contact with the EU Hybrid Fusion Cell"[37] has been improving coordination between NATO allies and EU member states on developing joint research, exchanging best practices, and conducting crisis management exercises. Its three research focuses are spearheaded by Finland, Germany, and the United Kingdom.[38]

29 Franklin D. Kramer, Hans Binnendijk, and Lauren M. Speranza, "NATO Priorities after the Brussels Summit," Atlantic Council, November 29, 2018, 12.

30 Sebastian Bay et al., "Responding to Cognitive Security Challenges," NATO StratCom Centre of Excellence, January 2019.

31 NATO Operational Experimentation, "Fact Sheet – Information Environment Assessment (IEA)," NATO Allied Command Transformation, March 2018, 1.

32 The President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, "Joint Declaration on EU-NATO Cooperation," North Atlantic Treaty Organization, July 10, 2018.

33 "Third Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017," North Atlantic Treaty Organization, June 8, 2018.

34 "EU Hybrid Exercise 2018: Strengthening European Crisis Response," European External Action Service, November 2018.

35 "About Us," NATO StratCom Centre of Excellence.

36 "What is Hybrid CoE?" Hybrid CoE.

37 "Foreign Influence Operations in the EU," European Parliament, July 2018.

38 "Communities of Interest," Hybrid CoE.

However, it is unclear to what extent the Helsinki center has bridged the two organizations' capabilities to tackle a common threat. Several members of both do not participate in its work. The center acknowledges the need to "move on from describing the threats to countering them."[39] Lastly, the center does not have a direct pipeline into NATO or EU decision-making structures, limiting its influence beyond facilitating staff to staff NATO-EU talks. It remains up to the participating states to leverage their engagement in the centers' activities.

National Governments

In addition to actions at the international level, individual European states have taken steps to safeguard their information ecosystems. Some countries like Germany, which is especially sensitive to hate speech due to historical reasons, or France, with its strong tradition of state intervention, see legislation as the best way to combat disinformation. However, some governments, the private sector, and civil society have also pursued other approaches, sometimes in conjunction with new laws, to counter foreign authoritarian information operations by developing expertise, raising awareness and building societal resilience.

Regulating the Information Space

As of November 2018, 15 EU or NATO member states were working on or had already passed legislation aimed at better regulating the online information space.[40]

The German Bundestag passed Europe's first such piece of legislation, the Network Enforcement Act (or NetzDG), in June 2017. It imposes new obligations on social networks to remove "illegal content" from their platforms within a set timeframe or face steep fines.[41] Under NetzDG, "illegal content" is broadly construed and includes incitements to hatred, depictions of violence, and child pornography, but also defamation and "forgery of data intended to provide proof."[42] Since the law was passed, the primary social networks have appointed points of contact to interact with the Ministry of Justice, receive inquiries, and operate channels dedicated to processing reports of "illegal content." The Ministry of Justice is monitoring the law's impact and plans to fully evaluate it by the end of 2020.

The German law raises two concerns. First, contrary to terrorist content, the content spread by state actors to mislead or inflame divisions is rarely so overtly inflammatory as to be considered criminal under NetzDG's definition of "illegal content." Second, critics of the law argue that its focus on the number of pieces of content taken down encourages social media companies to over-moderate and remove anything they fear could be construed as illegal.[43] For example, critics pointed to Twitter's banning of a leftwing politician for a satirical song taken out of context in January 2018 as an indication of companies' knee-jerk reaction to removing content that may run afoul of the law.[44] As of November 2018, the Ministry of Justice had yet to impose a fine on any company.

In France, the National Assembly passed the Law Against the Manipulation of Information in November 2018.[45] It requires online platforms to set up and publicly advertise measures to fight disinformation. In addition, the law empowers the national media regulator to suspend the broadcast of a television channel affiliated with a foreign government if it is deemed to be damaging to the national interest. Some fear, however, that the new law "will mostly just give the government more control over the media."[46]

The German and French legislative approaches to tackling disinformation focus on content. For historical reasons, these countries are more willing to ban certain ideas or types of speech from the public sphere in order to protect democracy. However,

39 Axel Hagelstam and Kirsti Narinen, "Cooperating to Counter Hybrid Threats," NATO Review, November 23, 2018.

40 Samantha Bradshaw, Lisa-Marie Neudert, and Philip N. Howard, "Government Responses to Malicious Use of Social Media," NATO StratCom Centre of Excellence, November 2018.

41 William Echikson and Olivia Knodt, "Germany's NetzDG: A Key Test for Combatting Online Hate," Center for European Policy Studies, November 22, 2018.

42 Echikson and Knodt, "Germany's NetzDG," 22.

43 Dietmar Neuerer, "Hasskommentare Werden Erst Nach 80 Tagen Gelöscht – Kampf Gegen Hetze Immer Schwieriger," Handelsblatt, March 6, 2018.

44 Freedom on the Net 2018, "Germany," Freedom House, 2018.

45 "Lutte Contre La Manipulation de L'Information," Gouvernement, République Française, last updated January 4, 2019.

46 Rim-Sarah Alouane, "Macron's Fake News Solution Is a Problem," Foreign Policy, May 29, 2018.

their attempts to determine what is and what is not acceptable content online pose risks to the protection of free speech. In this context, the United Kingdom's plan to emulate the content-centric approach of their continental counterparts is concerning.[47]

Concentrating on online behavior rather than on content avoids these potential risks to free speech. Information operations rely on trolls, people masquerading as concerned citizens, bots, and computer programs to amplify divisive content on social media. Trolls and bots give off certain signals highlighting their inauthentic nature; for instance, by posting at odd times or at superhuman frequencies. Legislation focused on sanctioning these forms of malign behavior would sidestep the issue of having to prove the ways in which specific pieces of content promoted by foreign authoritarian actors are harmful.

Online Political Advertisements

Information operations also use the advanced targeting tools offered to advertisers by social media companies to reach citizens particularly susceptible to certain messages. Targeting specific segments of the American public with inflammatory ads was one of the key methods Russian government operatives used to influence voters in the United States in 2016.[48] They took advantage of the platforms' lack of mechanisms for stopping malign actors who covertly purchased ads on their platform and masked their true identities in the process. The platforms also did not make information available to users about who was paying for the ads they were seeing and masking their identity in the process. Government regulation is needed to address this challenge, as the companies have proven unreliable to regulate themselves.

So far, two European states have attempted to regulate this space. France's law against information manipulation includes measures that apply only during electoral campaigns. These include imposing a duty on online platforms to signal sponsored content and publishing the names of those who paid for them as well as the amount they paid. In Ireland, the Online Advertising and Social Media (Transparency) Bill made it to the committee stage in the Dáil Éireann (the lower house of parliament) despite the government's opposition, where it has been stalled there since 2017.[49]

> *"The gaps in social media companies' implementation of political ad transparency should encourage national governments to intervene.*

Social media companies have also taken steps to allow their users to identify who is targeting them with political ads. Improving transparency of political advertising was one of the key objectives in the EU Code of Practice on Disinformation in the runup to the May 2019 European Parliament elections. In addition, beginning in April 2019, ahead of the elections, Facebook made available in the EU tools it had launched ahead of the 2018 U.S. midterm elections to make political ads on its apps more transparent. This included clearer labeling of who paid for ads and an archive with political ads placed on Facebook's various platforms.[50] Similar initiatives have been launched by Google,[51] and Twitter.[52]

However, these efforts suffered from timing and implementation issues. Crucially, they only became operational a few weeks before the European Parliament elections. By contrast, information operations often begin months, if not years, ahead of the event they seek to influence. In addition, social media companies adopted one-size-fits-all responses that failed to take European specificities into account. For instance, Facebook's new registration

47 Department for Digital, Culture, Media & Sport, Home Office, "Online Harms White Paper," UK Government, April 8, 2019, last updated April 30, 2019.

48 Philip Bump, "What Data on More Than 3,500 Russian Facebook Ads Reveals About the Interference Effort," The Washington Post, May 10, 2018.

49 James Lawless, "Online Advertising and Social Media (Transparency) Bill 2017," House of the Oireachtas, December 6, 2017, last updated December 14, 2017.

50 Richard Allan, "Protecting Elections in the EU," Facebook Newsroom, March 28, 2019.

51 "Political Advertising in the European Union," Google Transparency Report.

52 "Ads Transparency Center," Twitter.

requirements, which were meant to limit foreign authoritarian actors from disrupting the elections with misleading ads, ended up limiting the ability of pan-European parties and organizations to campaign across the entire EU.[53]

These gaps in social media companies' implementation of political ad transparency should encourage national governments to intervene. A good first step would be to follow France's lead to require social media companies to report who pays for political ads on their platforms and increase transparency about the criteria used to target users with these ads. Stronger collaboration between governments and the companies in identifying purchasers of political ads who conceal their affiliation with foreign authoritarian states would provide another layer of defense.

Building Resilience against Disinformation

Beyond legislative measures, European governments have implemented a variety of approaches to push back against disinformation. The Czech Republic,[54] Slovakia,[55] and the United Kingdom,[56] have created new teams specifically dedicated to strategic communications. In France, national experts embedded within social media companies have suggested a new framework for cross-cutting cooperation between these and the state.[57] Particularly notable is this framework's insistence on the role that should be played by non-state actors, be it in the private sector or civil society.

Finland,[58] France,[59] Italy,[60] and Slovakia[61] are among the countries that have launched anti-disinformation campaigns in schools. All these programs include media-literacy training; for instance, by teaching students how to determine whether a story is false or by encouraging them to cross-reference things they read online. The Finnish program, in particular, teaches more specialized skills, such as how to recognize a troll or bot by taking a closer look at their social media profile. The degree of governmental involvement in these programs varies from country to country but they all have the advantage of reaching a broader audience and of mobilizing civil society actors such as journalists and educators.

> "***Beyond social media companies, other private-sector initiatives have sought to contribute to the fight against disinformation.***

Beyond social media companies, other private-sector initiatives have sought to contribute to the fight against disinformation. For instance, NewsGuard uses journalists and other media experts to assess the reliability of online outlets in the United States and several European countries, and it condenses their findings into easy to understand "nutrition labels." Its assessment methodology is based on certain content-neutral criteria, such as an outlet's correction policy, or the availability of information about its content creators that any outlet can improve upon to get a better nutrition label.

The NGO Reporters Without Borders and its partners have proposed a different approach. The Journalism Trust Initiative puts journalists in charge of developing self-regulatory measures. Journalists

53 Mehreen Khan, "Facebook Signals Softer Stance on Ad Rules for EU Elections," Financial Times, April 21, 2019.

54 Robert Tait, "Czech Republic to Fight 'Fake News' with Specialist Unit," The Guardian, December 28, 2016.

55 Aktivity Štátnych Tajomníkov, "Prvé Stretnutie Medzirezortnej Koordinačnej Skupiny Pre Boj Proti Dezinformáciám a Strategickú Komunikáciu," Ministerstvo Zahraničných Vecí a Európskych Záležitostí, March 21, 2019.

56 Tom McTague, "How Britain Grapples with Nationalist Dark Web," Politico, December 17, 2018.

57 "Creating a French Framework to Make Social Media Platforms More Accountable: Acting in France with a European Vision," République Française, May 2019.

58 Eliza Mackintosh, "Finland is Winning the War on Fake News. What It's Learned May Be Crucial to Western Democracy," CNN, May 2019.

59 Adam Satariano and Elian Peltier, "In France, School Lessons Ask: Which Twitter Post Should You Trust?," The New York Times, December 13, 2018.

60 Horowitz, "In Italian Schools, Reading, Writing and Recognizing Fake News."

61 Kolektív Autorov, "Učitelia Proti Dezinformáciám," Slovak Security Policy Institute, January 2018.

would set up commonly agreed standards and the system would "reward media outlets for providing guarantees regarding transparency, verification and correction methods." This system would contribute to improved ethical norms and promote a multi-stakeholder approach to solving the disinformation problem.[62]

Civil society and journalists have created dozens of fact-checking organizations all over Europe that seek to correct false or misleading information published online.[63] While fact checking is costly and only reaches citizens after disinformation is spread, it adds another layer of defense to democracies' information space when used in combination with all the other initiatives already described.

Some European actors have been even more creative in their solutions to combat disinformation. A Dutch start-up has developed a videogame that demystifies the tools used by purveyors of disinformation by tasking players with producing such content.[64] In Sweden, the editors for one of the country's most famous comics decided to make several adventures of a popular character focus on teaching children about the importance of double-checking online sources.[65] Creating defenses against foreign interference activities is incumbent on all citizens and all sectors of democratic societies.[66]

62 "More Than 100 Media Outlets and Organizations are Backing the Journalism Trust Initiative."

63 Lucas Graves and Federica Cherubini, "The Rise of Fact-Checking Sites in Europe," Reuters Institute for the Study of Journalism, University of Oxford, November 2016.

64 "The Resistance to Disinformation," DROG.

65 Roden, "Why This Swedish Comic Hero is Going to Teach Kids About Fake News."

66 Nad'a Kovalcikova, "Beyond Elections' Digital Propaganda: Need for Improvement of Public Debates," American Institute for Contemporary German Studies, February 11, 2019.

ANNEX B. SECURING PROSPERITY WITHOUT LOSING INTEGRITY

Keeping Dirty Money Out

How Europe has Facilitated Malign Finance

Misappropriated public funds and corrupt proceeds often fund foreign authoritarian regimes' acquisitions and foreign direct investment (FDI). Major money-laundering schemes such as the Russian Laundromat,[1] which saw $20.8 billion coming from 19 Russian banks laundered through 5,140 companies with accounts in 732 banks in 96 countries, play a large role in enabling foreign authoritarian regimes' macroeconomic decisions. Corrupt elites set up shell corporations or use European and North American banks to siphon wealth from their countries, criminally enrich themselves, and finance nefarious activities for the benefit of the state. The U.K. House of Commons' Foreign Affairs Select Committee has found that "there is a direct relationship between the oligarchs' wealth and the ability of President Putin to execute his aggressive foreign policy and domestic agenda."[2]

The best-known example of this oligarch-state nexus is Yevgeny Prigozhin, "Putin's chef," who uses his wealth to finance the Internet Research Agency in St. Petersburg and to sponsor mercenary groups in Ukraine and Syria.[3] Another is Vladimir Yakunin, a close friend of President Vladimir Putin, who headed Russian Railways until his abrupt dismissal in 2015. Whistleblowers subsequently revealed that corruption was endemic in the state-owned consortium, which required almost $7 billion of Russian taxpayers' money to stay afloat in the years after Yakunin's removal.[4] Despite his crimes and U.S. sanctions that froze his assets, Yakunin is now based in Berlin, where he heads a pro-Kremlin think tank and gets invited to conferences partly funded by the EU.[5]

Large-scale money laundering scandals linked at least in part to Russia have erupted across Europe. They have occurred at banks in Cyprus, Estonia, Latvia, Malta, the Netherlands, and the United Kingdom, and have involved larger institutions headquartered in Denmark and Germany, such as Danske Bank and Deutsche Bank. This activity has amounted to hundreds of billions of dollars in recent years. The problem is exacerbated by the EU's financial supervisory architecture, in which financial services are spread across the single market and prudential supervision is centralized within the eurozone, while anti-money laundering oversight is left to national authorities. This setup makes coordination on cross-border activity difficult, leaves some of the smallest, lowest-capacity jurisdictions as the first line of defense, and encourages regulatory and political capture, especially in small countries with outsized financial sectors.[6]

The transnational nature of money laundering means that national regulators have sometimes failed to connect the dots quickly enough. This is what caused up to €200 billion ($227 billion) of suspicious payments to flow undetected through the Estonian

1 "The Russian Laundromat Exposed," Organized Crime and Corruption Reporting Project, August 22, 2014.

2 "Moscow's Gold: Russian Corruption in the UK," UK Parliament, May 21, 2018.

3 Pavel K. Baev, "New Russian Question: Who Is Mr. Prigozhin?" Eurasia Daily Monitor, The Jamestown Foundation, February 26, 2018.

4 Sergei Khazov-Cassia, "Russian Whistle-Blower Pulls Back Cover On Railways Corruption," RadioFreeEurope/RadioLiberty, October 10, 2016.

5 Etienne Soula, "Authoritarians' Latest Foothold in Brussels," Alliance for Securing Democracy, February 28, 2019.

6 Kirschenbaum and Véron, "The European Union Must Change Its Supervisory Architecture to Fight Money Laundering."

branch of Danske Bank between 2007 and 2015.[7] This case has triggered a strong response from all involved, with Denmark significantly strengthening its anti-money laundering framework[8] and Estonia shutting down the branch responsible for these transactions.[9]

How Europe is Fighting Back

The sensational nature of many of these money-laundering cases has compelled EU institutions and many member states to begin to address the systemic vulnerabilities that have enabled authoritarian regimes to move corrupt money into Europe. The EU made determining the beneficial ownership of companies a key objective of its 2015 Fourth Anti-Money Laundering (AML) Directive and continues to push for greater transparency across the financial sector. The Fourth Directive mandated that member states establish centralized registers of the beneficial owners of companies incorporated in the EU.[10] It also imposed a duty on EU financial institutions and intermediaries (lawyers, auditors, etc.) to conduct enhanced due diligence checks on customers hailing from "high-risk third countries."[11] Even before the Fourth Directive was fully implemented throughout the union, the EU moved forward with a Fifth Directive in response to the Panama Papers revelations of non-Europeans setting up bank accounts in Europe to avoid paying taxes at home. Crucially, the latest legislation obliges member states to make their registers of companies' beneficial ownership public and to create central registers of bank accounts.[12] The EU AML directives also set strong standards requiring member states to supervise financial institutions to ensure that they maintain robust anti-money laundering compliance programs to prevent and detect illicit activity.

These new measures have positioned the EU as a global leader on company registration transparency. When the Fifth Directive is fully transposed and implemented, it will significantly strengthen global anti-money laundering standards. The EU directives exceed international beneficial ownership standards set by the Financial Action Task Force, the intergovernmental organization that develops policies to combat money laundering. The EU's AML efforts suffered a setback when the European Council rejected a list of "high-risk third countries" proposed by the European Commission, according to which European financial institutions would be required to conduct more stringent checks and due-diligence tests when involved in transactions with entities from the listed countries; member states, the United States, and others objected to some of the entities on the list and the process of its adoption.[13]

> ***"The sensational nature of many money-laundering cases has compelled EU institutions and many member states to begin to address the systemic vulnerabilities that have enabled authoritarian regimes to move corrupt money into Europe.***

Some member states choose to go above and beyond the EU directives' requirement. The United Kingdom has been especially proactive in this arena. The Foreign Affairs Committee of the House of Commons recently published a scathing report on the role of the country in aiding and abetting Russia's aggressive foreign policy.[14] In 2016, the government

7 Teis Jensen, "Explainer: Danske Bank's 200 Billion Euro Money Laundering Scandal," Reuters, November 19, 2018.

8 "Agreement Between the Government (Venstre, Liberal Alliance and Det Konservativ Folkeparti) and Socialdemokratiet, Dansk Folkeparti, Radikale Venstre og Socialistisk Folkeparti on Further Initiatives to Strengthen Efforts to Combat Money Laundering and Terrorist Financing," Ministry of Industry, Business, and Financial Affairs, September 19, 2018.

9 "Estonia Orders Danske Bank Branch to Shut," BBC, February 19, 2019.

10 "Directive (EU) 2015/849 of the European Parliament and of the Council," Official Journal of the European Union, EUR-Lex, May 20, 2015, Chapter III.

11 Ibid., Section 3.

12 Policies, Information, and Services, "Anti-Money Laundering and Counter Terrorist Financing," European Commission.

13 Julia C. Morse, "The E.U. Tried to Blacklist Countries at High Risk for Money Laundering, But It Backfired. Here's Why," The Washington Post, March 14, 2019; "EU Commission Publishes 'Controversial' List of High-Risk Third Countries," DLA Piper, May 23, 2019.

14 "Moscow's Gold: Russian Corruption in the UK,"

set up a public register of beneficial ownership for companies owning property in the United Kingdom. The register currently only applies to U.K. companies, but a beneficial ownership register for overseas entities that own U.K. property is currently in the works.[15] With London real estate being a favorite destination for Russian oligarchs' (and, increasingly, wealthy Chinese investors') ill-gotten money,[16] the government should be pushing more strongly for increased transparency to prevent foreign authoritarian elites from sheltering their assets. The United Kingdom's efforts only scrape the surface of what needs to be done. About 15 percent of the country's land is still unregistered, meaning that the legal owner cannot be identified.[17]

> "*Some member states choose to go above and beyond the EU directives' requirement.*

Another country that has moved decisively against money laundering is the Netherlands. In September 2018, the Public Prosecution Service reached a $900 million settlement with ING Bank for money laundering offences committed between 2010 and 2016.[18] ING had notably enabled one of its clients, Vimpelcom, a Russian-owned telecommunications company, to pay more than €48 million ($55 million) of bribes to people related to a company owned by the daughter of the then-president of Uzbekistan.[19] What stands out in the Dutch authorities' action is that it was unprompted by outside reports or news stories and that the fine was an order of magnitude higher than those imposed on banks in similar cases in other EU member states.[20] While similar money scandals involving Russia have recently surfaced in Cyprus, Estonia, Latvia, and Malta, fines have remained in the single-digit millions. Still, the Netherlands is struggling in other areas. According to one study, Russian FDI "represented roughly 13 percent of Dutch nominal GDP in 2017, despite the fact that only around 20,000 people work for Russian-owned companies in the Netherlands."[21]

Keeping Dark Money Out of Elections

Some European nations have laws that allow foreign entities to finance political candidates, parties, and their campaigns. A review of election finance laws in all 28 EU member states showed that less than half had a full ban on foreign donations, with 11 having partial restrictions in place.[22] Those partial restrictions vary widely: Austria and Germany limit amounts that can be donated by anyone regardless of nationality, while Finland and Slovakia allow foreign donations from like-minded political parties. There are four countries with no restrictions in place—Belgium, Denmark, Italy, and the Netherlands. However, the Netherlands announced in January 2019 that it intends to ban political donations coming from countries outside of the EU.[23]

In March 2019, France's President Emmanuel Macron put forth his vision for a "European Renewal." One of his proposals was to "ban the funding of European political parties by foreign powers."[24] France itself demonstrated the difficulties involved in clamping down on foreign funding. Under French law, corporations, unions, and other collectives, most notably foreign governments, are prohibited from making donations to political parties.[25] But nothing stops parties from taking out loans with banks and there is no nationality requirement. This means that the loan Marine Le

15 Department for Business, Energy and Industrial Strategy, "Draft Registration of Overseas Entities Bill," UK Government, July 23, 2018, last updated April 18, 2019.

16 Joshua Chaffin, "Estate Agent to Rich Russians Rues London's Hostile Climate," Financial Times, May 30, 2018.

17 Adam Hookway, "Searching for the Owner of Unregistered Land," HM Land Registry, February 5, 2018.

18 National Office for Serious Fraud, Environmental Crime and Asset Confiscation (Functioneel Parket) and National Office (Landelijk Parket), "Investigation Houston: Criminal investigation into ING Bank N.V. - Statement of Facts and Conclusions of the Netherlands Public Prosecution Service," Netherlands Public Prosecution Service.

19 Ibid.

20 Joshua Kirschenbaum, "Europe Needs Money Laundering Penalties That Hurt," Alliance for Securing Democracy, September 12, 2018.

21 Heather A. Conley, Donatienne Ruy, Ruslan Stefanov, and Martin Vladimirov, "The Kremlin Playbook 2," Center for Strategic and International Studies, March 2019.

22 Berzina, "Foreign Funding Threats to the EU's 2019 Elections."

23 "Giften Van Buiten de EU Aan Politieke Partijen Mogen Niet Meer."

24 Emmanuel Macron, "For European Renewal," Élysée, March 4, 2019.

25 "Comment Les Parties Sont-ils Financés?" Direction de L'information Légale et Administrative, January 14, 2018.

Pen's far-right National Rally (formerly National Front) party received from First Czech-Russian Bank in 2016 was legal under French law.

> *"The European Parliament has been pushing the European Commission to investigate "golden visa" schemes since 2014.*

More recently, the Italian press revealed that the far-right Lega party may have been in talks with influential Russians to obtain funding for its European Parliamentary campaign. Italy is one of the EU countries with no limit on foreign funding, so Russian financial support to Lega may very well be legal under Italian law. This case is made more complicated because the funding allegedly would have been made through an opaque gas purchase agreement.[26] If anything, the Italian election financing system has been made more vulnerable in recent years as public funding available to parties was phased out between 2014 and 2017,[27] which opens space for other sources of funding.

Reassessing Visa and Passport Schemes

Related to the above-mentioned anti-money laundering efforts, the EU has been looking into so-called "golden passports" and "golden visa" schemes introduced by several member states. With the financial crisis weighing on many nations' balance sheets, some have encouraged foreigners to invest in their countries in exchange for visas and passports valid in the entire EU. With such documents, agents of foreign authoritarian regimes are free to circulate within the EU unencumbered. Only Bulgaria, Malta, and Cyprus currently grant citizenship to investors via "golden passports," but 20 EU member states grant the right of residence, via "golden visas," to foreigners on the basis of investment in the country.[28] In many cases, residing in the country for several years can help these investors apply for citizenship further down the line.

Golden visa schemes vary widely from country to country.

- The required investment varies from no financial threshold in Greece and Poland, to €5 million in Slovakia and Luxembourg.[29]
- The type of investment required is not always the same.[30] Countries like Cyprus, Portugal, and Spain require a real estate transaction of a certain value. Others such as Hungary and Italy require an investment in government bonds. Malta and Latvia ask for a one-time contribution to the state budget.
- The duration and renewal of the residence permit ranges from six months in Bulgaria and Spain, to ten years in Greece.[31]

Vetting of investors is similarly uneven. The European Commission is unable to ascertain precisely which security checks, if any, are conducted by some of the member states: Bulgaria, Italy, Latvia, Lithuania, Slovakia, and Slovenia.[32]

The European Parliament has been pushing the European Commission to investigate these schemes since 2014.[33] While determining who is and is not a country's citizen is a national matter, the European Commission's latest report on investor citizenship makes it very clear that "granting naturalization based on a monetary payment alone […] affects citizenship of the Union."[34] These schemes can directly affect

26 Barbie Latza Nadeau, "An Italian Expose Documents Moscow Money Allegedly Funding Italy's Far-Right Salvini," The Daily Beast, February 22, 2019.

27 OSCE/ODIHR Needs Assessment Mission Report, "The Italian Republic Parliamentary Elections: 4 March 2018," OSCE Office for Democratic Institutions and Human Rights, February 1, 2018, 10.

28 "Questions and Answers on the Report on Investor Citizenship and Residence Schemes in the European Union," European Commission, January 23, 2019.

29 Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Commission Staff Working Document: Investor Citizenship and Residence Schemes in the European Union," European Commission, January 23, 2019, 18.

30 Ibid., 15.

31 Ibid., 20.

32 Ibid., 22.

33 "EU Citizenship for Sale," European Parliament, January 16, 2014.

34 Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Investor Citizenship and Residence Schemes in the European Union," European Commission, January 23, 2019, 6.

the EU's ability to fight money laundering. Under the Anti-Money Laundering Directives, financial institutions are not required to be as rigorous in their due-diligence checks when the investor is from one of the EU member states. This means that countries with lax investor visa schemes open the entire EU to opaque funding from authoritarian regimes. The European Commission is looking to counter the influence of these schemes and will soon establish a group of experts who will issue recommendations on addressing the risks posed by investor passports and monitor the implementation of EU law in the context of investor visas.[35]

Pushing Back Against Strategic Economic Coercion

Overcoming Corruption and Coercion in the Energy Sector

Europe's energy markets are vulnerable to corruption, coercive investments, and political influence, especially in the natural gas and nuclear sectors. This vulnerability directly affects the ability of Europeans to keep their lights on and heat working, but it also feeds larger political divisions between EU member states. The EU has made progress in creating a single political and physical European energy market that bolsters the power of smaller, more vulnerable Central and Eastern European member states. This was a significant step, as some countries had been wholly reliant on Russia for their natural gas (and often other fuel) supplies as a result of the infrastructure and economic legacy of the Soviet Union. Yet, energy remains a powerful lever of Russia's malign influence. Russia and European companies and countries are still moving forward with pipeline projects like Nord Stream 2, which pit the interests of smaller EU states against big ones.

Russia is the largest supplier of natural gas to the EU[36] and has used its dominant position either to punish European states, including Ukraine, or to reward friendly governments.[37] The interruption of natural gas flows to Europe in 2006 and 2009 turned off heat across the continent and pressed the EU to start legislating to protect the continent's security of supply. The Electricity and Gas Directives of the Third Package—major pieces of legislation that seek to separate energy generation from distribution and sales to improve competition—contain provisions that allow EU member states to deny certification to projects run by non-EU countries when they fear and substantiate their concerns that these will harm the security of supply.[38]

Equally troubling, but less visible, are non-transparent agreements that Russian state-controlled or state-linked companies have concluded below market value that increase the Russian government's leverage over target countries. These agreements have isolated EU member states and hindered the creation of a more secure and competitive EU-wide gas market.[39] The European Commission brought an antitrust case against Gazprom's practices in eight member states to eliminate these vulnerabilities and achieved concessions, though no fines, from Gazprom.[40]

As Europe's domestic natural gas reserves decline, imports from Russia are likely to increase. Since 2014, EU institutions and many member states have sought to make sure that dependence on Russian energy resources does not increase the risk of coercion. There are political and technical dimensions to this. Under President Jean-Claude Juncker, the European Commission has given significant weight to the question of energy security by designating a commissioner as a vice president in charge of the high-profile Energy Union project.[41] Politically, the project has been important for bolstering the common EU energy interest. Vice President Maroš Šefčovič has played a crucial foreign policy role by chairing gas delivery and transit negotiations

35 "Questions and Answers on the Report on Investor Citizenship and Residence Schemes in the European Union."

36 "EU Imports of Energy Products - Recent Developments," EuroStat, October 2018.

37 "Authoritarian Interference Tracker."

38 "Directive 2009/72/EC of the European Parliament and of the Council," Official Journal of the European Union, EUR-Lex, July 13, 2009.

39 "Antitrust: Commission Sends Statement of Objections to Gazprom for Alleged Abuse of Dominance on Central and Eastern European Gas Supply Markets," European Commission, April 22, 2015.

40 "Authoritarian Interference Tracker."

41 "Energy Union and Climate," European Commission.

between Ukraine and Russia[42] and working with the United States to support efforts to bring liquefied natural gas (LNG) to Europe.[43]

The Energy Union has achieved impressive technical solutions. New reverse-flow capabilities allow EU member states to send gas east. This not only protects these countries, but also allows Ukraine to buy its natural gas from the EU rather than from Russia directly.[44] This technical capacity dovetails with the achievements of the Gazprom anti-trust case (the elimination of destination clauses) and allows member states to share their natural gas supplies.

The European Commission has accomplished other measures too.

- Stress tests have checked the gas sector's resilience to interruptions and allowed member states to plan contingencies in case of outages.[45]
- A new Regulation on Security of Gas Supply, which entered into force in the fall of 2018, requires member states to carry out risk assessments of how non-EU control of infrastructure may affect security of supply.[46]
- EU funds are supporting the creation of LNG import terminals and pipeline interconnections to eliminate vulnerabilities.[47]

Earlier this year, the European Commission extended the EU's internal gas market rules to make them applicable to future pipelines between member states and third countries, though existing pipelines may be exempt.[48]

42 Alissa de Carbonnel, "UPDATE 2-Russia, Ukraine to Hold Further Gas Talks in May," Reuters, January 21, 2019.

43 "Vice-President Šefčovič Joins U.S. President Trump in Opening an LNG Export Terminal," European Commission, May 14, 2019.

44 European Parliamentary Research Service and Directorate-General for External Policies, "The Quest for Natural Gas Pipelines," European Parliament, July 2016.

45 "Stress Tests: Cooperation Key for Coping with Potential Gas Disruption," European Commission, October 16, 2014.

46 "Regulation (EU) 2017/1938 of the European Parliament and of the Council," Official Journal of the European Union, EUR-Lex, October 25, 2017, 1–56.

47 "Projects of Common Interest," European Commission.

48 "Council Adopts Gas Directive Amendment: EU Rules Extended to Pipelines To and From Third Countries," Council of the European Union, April 15, 2019.

But even an initiative as significant as the Energy Union has not been able to overcome the coercive impact that the long-term energy ties with Russia have had on EU politics. The Nord Stream 2 project, which will expand an existing gas pipeline from Russia to Germany, pits EU member states against each other. The European Commission's new gas rules do not apply to the project, and Germany has the decisive say in whether the pipeline project goes forward.[49] The project allows Russian state-controlled energy companies to undermine European solidarity because of perceptions that it benefits Germany at the cost of other member states.

> *"Since 2014, EU institutions and many member states have sought to make sure that dependence on Russian energy resources does not increase the risk of coercion.*

Russia also uses energy politics to gain political leverage by coopting local actors and to build long-term influence. Germany's former chancellor, Gerhard Schroeder, supported plans for Nord Stream 2 while he was in office. After leaving office, he became chairman of Nord Stream's shareholders' committee, and in 2017, joined the board of Rosneft, the Russian state-controlled oil company. Schroeder is also the chairman of Nord Stream 2's shareholders' committee.[50]

According to ASD's Senior Fellow on Malign Finance Joshua Kirschenbaum, aside from the high profile cases like Nord Stream, Russia uses "energy delivery intermediaries, often based in Switzerland, to enrich favored elites in consumer countries; [...]

49 Frédéric Simon, "EU Strikes Deal on Rules to Govern Russia's Nord Stream 2 Pipeline," Euractiv, February 13, 2019.

50 "Anger as German Ex-Chancellor Schroeder Heads Up Rosneft Board," BBC, September 29, 2017.

energy firms to conduct political financing designed to influence the political affairs of consumer countries" and makes "politically driven energy decisions" about natural gas and nuclear power.[51] In Hungary, for example, oligarchs allied with Viktor Orbán earned hundreds of millions of dollars buying discounted Gazprom gas through a Swiss trading firm and reselling it in Hungary at market prices. The scheme enriched Orbán's allies at Hungarian citizens' expense.[52]

Nuclear power is increasingly an alternative to gas that Russia uses to extend its energy influence. Four EU member states and Ukraine are dependent on the country to supply nuclear fuel to their Russian-built nuclear reactors.[53] Russia's influence in this sector is growing. Hungary granted the Russian state corporation Rosatom a contract to expand a nuclear power plant without an open tender and without any public oversight. The country's parliament voted to keep most details of the agreement a state secret for 30 years.[54]

> "*European states are growing more concerned about FDI emanating from companies closely tied to authoritarian regimes, notably China's.*

Clearly, Europe still has divergent views regarding energy dependence on Russia. Given the long-term nature of energy investments, Russia's influence in the energy sector will be present for the foreseeable future. Technical solutions are preventing blackouts and price gauging, but new energy deals are extending political dependencies on Russia. Perhaps a new framework for FDI screening would further protect the EU energy infrastructure from foreign authoritarian maneuvers.

Scrutinizing Chinese investments: Strategic Sectors and FDI

European states are growing more concerned about FDI emanating from companies closely tied to authoritarian regimes, notably China's. Over the past decade, Chinese FDI into Europe has increased tenfold, with a peak of €37.2 billion in 2016.[55] By comparison, EU FDI into China has stabilized at around €10 billion per year since 2010.[56] By themselves, these numbers do not tell the full story of Europe's vulnerability. FDI from China has targeted strategic sectors and areas of new technological development. In early 2019, the 28 EU member states took the first step toward an EU-wide FDI screening process.

European governments have reason to be worried about high investment flows from the China. The Chinese government has an objective of achieving dominance in many high-tech fields of the economy by 2025 and will use government subsidies, make use of state-owned enterprises, and acquire intellectual property to achieve that aim.[57] Tellingly, European companies would be replaced or blocked from making in China many of the investments that Chinese companies have made in Europe,[58] though European resources and interest in such investments exist. While the share of investments made by Chinese state-owned enterprises has declined to 2016 levels, these vehicles are still responsible for a large part of Chinese FDI into Europe.[59] Furthermore, the fact that Chinese law compels private companies to cooperate with the government upon request, as well as the high level of coordination sometimes exhibited

51 Alliance for Securing Democracy and C4ADS, "Illicit Influence – Part Two – The Energy Weapon," The German Marshall Fund of the United States, April 25, 2019.

52 Dániel Hegedüs, "The Kremlin's Influence in Hungary: An Examination of Budapest's Ties to Moscow," Deutsche Gesellschaft für Auswärtige Politik/German Council on Foreign Relations, February 2016.

53 "Ensuring Europe's Nuclear Fuel Supply."

54 "Austria Sues Over EU Approval of Hungary Nuclear Plant," Euractiv, February 23, 2018.

55 Thilo Hanemann, Mikko Huotari and Agatha Kratz, "Chinese FDI in Europe: 2018 Trends and Impact of New Screening Policies," Rhodium Group and the Mercator Institute for China Studies, March 2019, 10.

56 Thilo Hanemann and Mikko Huotari, "EU-China FDI: Working Towards Reciprocity in Investment Relations," Rhodium Group and the Mercator Institute for China Studies, May 2018, 16.

57 McBride and Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?"

58 Hanemann and Huotari, "EU-China FDI: Working Towards Reciprocity in Investment Relations,"15-17.

59 Hanemann, Huotari, and Kratz, "Chinese FDI in Europe: 2018 Trends and Impact of New Screening Policies," 14.

by supposedly unrelated companies suggests a significant porousness between the Chinese private and public sectors.

China is by no means the only foreign authoritarian power with a worrying economic presence in Europe. Russia has also used investments and acquisitions to expand its influence in several countries. The Russia expert Ognian Shentov has found that "the tools the Kremlin has used in expanding its influence in critical economic sectors are not new to the [Central and Eastern European] region—political corruption, corporate raiding, and acquisition of strategic assets."[60] However, Russian economic influence is also present in other member states. One study found that Austria turns a blind eye to Russia's use of its "extensive banking and energy networks in CEE."[61] In May 2019, the Austrian government fell after a tape showed Vice-Chancellor Heinz-Christian Strache, who was also chairman of the far-right Freedom Party, meeting with someone he thought was the niece of a Russian oligarch. Strache offered the woman lucrative state contracts in exchange for her buying an Austrian tabloid and turning its editorial line to support the Freedom Party.[62]

However, it was increased investments by Chinese entities, particularly by state-owned enterprises, in European high-tech companies that drove France, Germany, and Italy, to call on the European Commission to develop a proposal for EU-wide action on investment screening.[63] The resulting "[r]egulation establishing a framework for the screening of foreign direct investments into the Union" formally passed into law in March 2019.[64] The regulation covers investments that target "critical technologies […] including artificial intelligence, robotics, semiconductors, [and] cybersecurity." Importantly, it also looks at investments affecting "the freedom and plurality of the media."[65]

> *"The fact that the EU opinions will be non-binding means that effective investment screening in the union still relies on the individual national mechanisms.*

The EU regulation is a binding legislative act that must be applied in its entirety across the union. The powers it grants to institutions are, however, relatively modest. It establishes a mechanism for information sharing on ongoing FDI screening processes between member states, and with the institutions.[66] The European Commission will be competent to assess incoming FDI, but its opinions will be non-binding and only applicable "if an FDI in a Member State may affect the security or public order of projects or programmes "of Union interest" or if an FDI in a Member State may affect the security or public order of other Member States."[67] The fact that the EU opinions will be non-binding means that effective investment screening in the union still relies on the individual national mechanisms. At present, only 14 EU member states have some form of investment-screening legislation.[68] Hopefully, the guidelines contained in the EU regulation will encourage more to set up their own mechanisms.[69]

60 Ognian Shentov, "The Russian Economic Grip on Central and Eastern Europe," Routledge, 2019.

61 Conley, Ruy, Stefanov, and Vladimirov, "The Kremlin Playbook 2," 14.

62 Zia Weise, "Austrian Far-Right Leader Filmed Offering Public Contracts for Campaign Support," Politico, May 17, 2019.

63 Yann Le Guernigou and Leigh Thomas, "France, Germany, Italy Urge Rethink of Foreign Investment in EU," Reuters, February 14, 2017; Valbona Zeneli, "Mapping China's Investments in Europe," The Diplomat, March 14, 2019.

64 "Foreign Investment Screening: New European Framework to Enter Into Force in April 2019," European Commission, March 5, 2019.

65 "Regulation of the European Parliament and of the Council Establishing a Framework for the Screening of Foreign Direct Investments into the Union," European Commission, February 20, 2019, Art.4

66 Ibid., Art.6

67 "Legislative Train Schedule: A Balanced and Progressive Trade Policy to Harness Globalisation – Screening of Direct Foreign Investment in Strategic Sectors."

68 Gisela Grieger, European Parliamentary Research Service "EU Framework for FDI Screening," European Parliament, February 2019.

69 Ibid., Art.3

There has been significant investment activity in several member states. For instance, Chinese acquisitions in the robotics sector have prompted Germany to revise and tighten its national investment-screening rules.[70] In July 2017, an amendment to the Foreign Trade Regulation was adopted to allow the government to screen and ultimately block a wider range of foreign takeovers.[71] In December 2018, the threshold for deals to be subject to ministerial veto

> *"All these legal developments will help EU member states protect their economies from the strategic acquisitions of states like China. However, the national schemes still lag behind the economic defenses put in place in the United States.*

was lowered from 25 percent to 10 percent of equity by a non-EU company.[72] Considering that German companies account for a very large proportion of the €198 billion exported by the EU to China yearly,[73] it is remarkable to see the Federation of German Industries being relatively supportive of a more assertive approach toward China.[74]

Other EU member states have also moved to strengthen their investment screening processes. In France, a large omnibus bill currently going through the parliament[75] proposes to strengthen the existing process, while executive orders are intended to expand its application to high-value sectors such as artificial intelligence, space, data storage, and semiconductors.[76] In July 2018, the U.K. government published a report advocating stronger powers to mitigate "the exploitation of acquisition of control or influence over U.K. entities or assets."[77] Other countries such as Belgium, the Czech Republic, Greece, the Netherlands, Slovakia and Sweden are also considering strengthening investment review mechanisms.[78]

All these legal developments will help EU member states protect their economies from the strategic acquisitions of states like China. However, the national schemes still lag behind the economic defenses put in place in the United States. The Committee on Foreign Investment in the United States (CFIUS) has been reformed and is now one of the most robust investment screening mechanisms in the world.[79] Through the CFIUS, an inter-agency and inter-disciplinary panel constantly monitors critical sectors of the economy and scrutinizes foreign investment directed at those sectors. Contrary to the EU's system, the CFIUS has the authority to impose conditions, or even to block, investments it deems dangerous for national security. Naturally, the fact that national security is by definition outside the remit of the EU's competences limits its ability to emulate the U.S. set-up. Nevertheless, the range of sectors considered critical by the European Commission is slightly larger than those within the CFIUS's purview and, if supported by robust national mechanisms, the EU's new regulation could yet effectively protect its members from foreign authoritarian strategic economic coercion.

70 Srinivas Mazumdaru, "Is Angst About China Behind Germany's Stricter Foreign Investment Rules?" Deutsche Welle, December 18, 2018.

71 "Investment Reviews," Federal Ministry for Economic Affairs and Energy.

72 "Zwölfte Verordnung zur Änderung der Außenwirtschaftsverordnung," Verordnung der Bundesregierung, December 6, 2018, Art. 1.

73 "Infographic - The EU and China are Strategic Trading Partners," Council of the European Union, 2018.

74 "Strengthen the European Union to Better Compete with China," BDI, January 10, 2019.

75 "Loi n° 2019-486 du 22 Mai 2019 Relative à la Croissance et la Transformation des Entreprises," Entreprise : Croissance et Transformation, Assemblée Nationale, May 23, 2019.

76 "Extension of the 2014 Decree: Better Protect French Strategic Companies," The Portal of Economy, Finance, Action and Public Accounts, République Française, February 19, 2018.

77 Secretary of State for Business, Energy and Industrial Strategy, "National Security and Investment: A Consultation on Proposed Legislative Reforms," UK Parliament, July 2018.

78 "Chinese FDI into North America and Europe in 2018 Falls 73% to Six-Year Low of $30 Billion," Baker McKenzie, January 14, 2019.

79 Stephanie Zable, "The Foreign Investment Risk Review Modernization Act of 2018," Lawfare, August 2, 2018.

ANNEX C. SECURING DIGITAL INFRASTRUCTURE AND MAKING TECHNOLOGY SAFE FOR DEMOCRACY

Today's Challenge: Strengthen Cybersecurity

The Emerging EU Framework

In July 2016, the EU published the directive on security of network and information systems (NIS Directive). It provides an EU framework within which national cyber authorities and capabilities can be pooled. The directive requires each member state to designate a computer security incident response team, also known as computer emergency response teams, and a competent national NIS authority.[1] Connecting these national authorities is meant to enable countries with more advanced cyber capabilities to assist the others by sharing expertise, good practices and lessons learned, and by developing common cybersecurity standards. Every member state has designated a competent national authority. Together with representatives of the European Commission and of the European Union Agency for Network and Information Security (ENISA), they form a Cooperation Group that facilitates strategic coordination.[2]

The first major document to have been published by this Cooperation Group is the Compendium on Cyber Security of Election Technology.[3] This draws examples of good practice from national case studies. These included measures taken by different countries at different stages of the electoral process such as: the training provided by French cyber authorities to political parties ahead of the election, the Czech and Dutch practice of conducting penetration testing on their electoral systems, the German decentralized voter registration process, the Estonian and Spanish task forces designated to oversee the smooth running of the vote, and the strict procedure for reporting election results in Austria.[4]

To further solidify its cyber framework, the EU adopted a new Cybersecurity Act in April 2019.[5] This expands the mandate and competencies of ENISA, in particular by giving it more operational responsibility to help coordinate the different national NIS authorities. The law also created an EU-wide certification framework for information communications technology products and services.[6]

A 2008 EU directive also helps member states identify and protect their critical infrastructure, mainly in the transport and energy sectors.[7] However, the risk of disruption to critical infrastructure by means of a cyberattack has significantly increased since 2008.[8] Foreign authoritarian governments have been tied to attacks on power plants,[9] financial institutions,[10] and

1 "Directive (EU) 2016/1148 of the European Parliament and of the Council," Official Journal of the European Union, EUR-Lex, July 7, 2016.

2 Ibid.

3 NIS Cooperation Group, "Compendium on Cyber Security of Election Technology," European Commission, March 2018.

4 NIS Cooperation Group, "Compendium on Cyber Security of Election Technology."

5 "EU Cybersecurity Agency (ENISA) and Information and Communication Technology Cybersecurity Certification (Cybersecurity Act)," Legislative Observatory, European Parliament, April 17, 2019.

6 "The Cybersecurity Act Strengthens Europe's Cybersecurity," European Commission, March 19, 2019.

7 "Council Directive 2009/114/EC," Official Journal of the European Union, EUR-Lex, December 8, 2008.

8 P. Gattinesi, "European Reference Network for Critical Infrastructure Protection: ERNCIP Handbook 2018 Edition," JRC Technical Reports, European Commission, May 31, 2018, 16.

9 Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," The Wall Street Journal, July 23, 2018.

10 Yalman Onaran, "North Korea Hackers Tried to Take $1.1 Billion in Bank Attacks," Bloomberg, October 8, 2018.

"residential routers worldwide."[11] In the United States, regulation has evolved, and even electoral systems are now designated as critical infrastructure.[12] So it is a step in the right direction that the European Commission is currently undertaking a systematic evaluation of the 2008 directive.[13]

> "The EU is limited in what it can do in the realm of cybersecurity because this is a national competence under EU law.

Lastly, in its most assertive action in this field to date, the European Council issued a May 2019 decision that would entitle the EU to impose countermeasures on persons or entities responsible for cyberattacks against the EU itself, a member state, and even third states and international organizations.[14] Possible sanctions include visa bans, asset freezes, and deprivation of funding from any EU person or entity. While this new measure sends an important deterrent signal to adversaries, how the policy will be implemented remains an open question because it would require consensus among member states to attribute an attack to a particular adversary. Individual states have already attributed cyberattacks to foreign authoritarian states, but the EU has yet to collectively attribute a government-sponsored cyberattack to a particular actor.[15]

The EU is limited in what it can do in the realm of cybersecurity because this is a national competence under EU law. In addition to lacking a broad mandate, EU institutions do not have their own cyber capabilities and largely rely on seconded national experts. Moreover, the EU's status as an international organization limits its ability to develop the norms for responsible state behavior in cyberspace. That conversation is currently taking place at the United Nations, where the United States and its allies support the Group of Governmental Experts process while a Russian resolution has given birth to a competing working group, with a barely concealed intent to increase state control online.[16] While the EU is supportive of the process,[17] it must stay on the sidelines as only national governments can participate in the group's work directly.

The Role of NATO and Cooperation with the EU

The EU is not the only organization working to improve cybersecurity in Europe. NATO has similarly recognized the threat posed to the alliance's security by cyberattacks conducted by foreign authoritarian states

At the Warsaw Summit of 2016, NATO officially recognized cyberspace as a "domain of operations." This means that the alliance must defend itself in cyberspace "as effectively as it does in the air, on land and at sea."[18] That recognition also allows allies to invoke Article 5 of the Washington Treaty in response to a cyberattack. Allies also signed the Cyber Defence Pledge that made upgrading their cyber defenses "a matter of priority." In a strong show of resolve, in May 2019 Secretary General Jens Stoltenberg declared that the alliance would not limit itself to cyber means when responding to a cyberattack.[19] NATO is currently in the process of staffing a cyber command to deter hackers and develop offensive cyber capabilities. It should be fully operational by 2023.[20]

11 "Alert (TA18-106A): Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices," Cybersecurity and Infrastructure Security Agency, Department of Homeland Security, April 16, 2018, last updated April 20, 2018.

12 European Political Strategy Centre, "Election Interference in the Digital Age: Building Resilience to Cyber-Enabled Threats," European Commission, October 16, 2018.

13 "Evaluation of the 2008 European Critical Infrastructure Protection Directive," European Commission, April 10, 2018.

14 "Council Decision Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States."

15 Paul Ivan, "Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox," European Policy Centre, March 18, 2019.

16 Alex Grisby, "The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased," Council on Foreign Relations, November 15, 2018.

17 "EU-U.S. Cyber Dialogue - Joint Elements Statement," European Union External Action Service, October 16, 2018.

18 "Cyber Defence," North Atlantic Treaty Organization, July 16, 2018.

19 Jens Stoltenberg, "Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London," North Atlantic Treaty Organization, May 23, 2019.

20 Robin Emmott, "NATO Cyber Command to be Fully Operational in 2023," Reuters, October 16, 2018.

NATO also contributes to European cybersecurity through its accreditation of the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. The center is sponsored by 21 nations, including members from both the EU and NATO. While most of its work is classified, it also contributes useful research and expertise to the European cybersecurity ecosystem. For instance, the Tallinn Manual 2.0, published in 2017 under the leadership of the center, is considered one of the most influential resources in Europe for national and international legal advisers who deal with cyber issues.[21] Every year, the center also hosts Locked Shields, one of the world's most sophisticated cyber defense exercise. This is "a unique opportunity to encourage […] training and cooperation between members of the [Tallinn Centre], NATO and partner nations."[22]

> "*With much of the authoritarian cyber threat directed at systems not traditionally considered "defense assets," including voting infrastructure, interior ministries, rather than defense ministries, are becoming more integral players in cybersecurity.*

With much of the authoritarian cyber threat directed at systems not traditionally considered "defense assets," including voting infrastructure, interior ministries, rather than defense ministries, are becoming more integral players in cybersecurity. This makes cooperation on cybersecurity between NATO and the EU more important than ever. NATO has identified cyber defense as one of the areas where cooperation with the EU has to be enhanced.[23] Since then, the two organizations have stepped up their cooperation and conducted common training and research, improved information sharing. They now regularly exchange best practices on cyber threats through regular meetings and "active interaction at staff level."[24] Finland and Ireland, EU members but not part of NATO, were included in the alliance's large yearly cyber exercise in 2018.[25] In June 2018, the European Parliament urged "EU member states […] to strengthen cyber cooperation at EU level, with NATO and other partners."[26]

National Efforts to Improve Cybersecurity

While the EU and NATO are developing frameworks for cooperation and coordination in cyberspace, cyber capabilities are still firmly in the hands of national governments.

All EU, NATO, and partner states now have at least one government arm in charge of improving cybersecurity, and in many cases have teams dedicated to protecting critical infrastructures.[27] This has fostered the development of holistic cyber strategies in many European states. For instance, Germany has developed the IT Baseline Protection framework to provide all information-handling actors in Germany with standards and procedures, supported by a certification scheme, "to achieve an appropriate security level."[28] In addition, German authorities and experts are currently debating to what extent, if at all, the latest iteration of Germany's cyber defense strategy should reserve the option to use cyber capabilities offensively.[29] Lithuania's five-year National Cyber Security Strategy lays out the country's plan to strengthen its cybersecurity and to develop its

21 "Tallinn Manual 2.0," The NATO Cooperative Cyber Defence Centre of Excellence, 2017.

22 "Locked Shields," The NATO Cooperative Cyber Defence Centre of Excellence, 2019.

23 "EU-NATO Cooperation – Factsheet," European External Action Service, June 11, 2019.

24 "EU-NATO Cooperation," European External Action Service, June 2019, 2.

25 Alexandra Brzozowski, "NATO Braces its Cyber Warriors Against Hybrid Threats," Euractiv, November 30, 2019.

26 "MEPs Want Robust EU Cyber Defence and Closer Ties with NATO," News, European Parliament, June 13, 2018.

27 "CSIRTs by Country – Interactive Map," European Union Agency for Network and Information Security.

28 "IT-Grundschutz," Federal Office for Information Security.

29 Alicia Prager, "Germany's Cyber Defence Strategy Discussed Behind Closed Doors," Euractiv, June 4, 2019.

cyber capabilities by 2023.[30] Meanwhile, an Estonian initiative to establish a network of cyber-volunteers who supplement the government's own personnel[31] has inspired Latvia[32] and France[33] to encourage volunteers to support national cyber troops.

Lastly, the private sector is also contributing to enhancing cybersecurity in Europe. Google offered in-person training to "most vulnerable groups" and provided free services to protect "news sites and free expression" from distributed denial of service attacks ahead of and during the recent European Parliament elections.[34] Similarly, Microsoft has expanded its cybersecurity program to 14 EU countries. Through this initiative, the company offered cybersecurity training and services to those taking part in the debates surrounding the elections, from political parties to think tanks.[35]

Navigating Digitization and Its Implications for Democracies

Decisive, but Controversial Action on Data Protection

As governments try to keep up with today's threats to IT systems, digitization is leading more people to conduct more activities online. The EU estimates that the monetary value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020.[36] This growing amount of personal data is handled by an also increasing number of entities. As that number grows, so does the risk that personal data ends up in the wrong hands. The Cambridge Analytica scandal, which revealed that a U.K. company had siphoned the data of millions of Facebook users and used it for political advertising, shows how malign actors could misuse this valuable commodity.

The EU's latest overhaul to its data protection law is the General Data Protection Regulation (GDPR), which entered into force in May 2018. Its most prominent clause requires entities to obtain explicit consent before processing an individual's personal data.[37] This condition is accompanied by several user rights, such as the right to know if, how, and why an individual's data is being processed by a service they use.[38] The GDPR also compels data processing entities to collect as little data as possible, to appoint employees specifically dedicated to data protection, and to notify users in case of a data breach.[39] Non-compliance triggers hefty fines. A data-processing entity found to have violated the regulation's provisions can be banned from processing user data further and fined up to several millions of euros.[40]

Although the GDPR is an EU initiative, its practical implementation and enforcement still largely relies on individual member states. The main point of contact for any question related to data protection is each country's data protection authority (DPA). Cooperation between DPAs and other national authorities, such as election officials, needs to be institutionalized. This may be complicated by the fact that many DPAs are underfunded and understaffed.[41] The authorities' lack of resources might be a contributing factor to relatively mild enforcement of the GDPR. France, whose regulator is committed to enforcing the regulation strictly, [42] was the only country as of May 2019 to have imposed a fine in the millions of euros.[43] Moreover, it is not the internet giants, but smaller companies that have been most likely to be fined by DPAs.[44]

30 "Resolution on the Approval of the National Cyber Security Strategy," Government of the Republic of Lithuania, August 13, 2018.

31 "Cybersecurity," Bloomberg.

32 Ģederts Ģelzis, "Latvia Launches Cyber Defence Unit to Beef Up Online Security," Deutsche Welle, March 4, 2014.

33 "Les Réserves de Cyberdéfense," Prévention des Risques Majeurs, République Française.

34 Lie Junius, "Supporting the European Union Parliamentary Elections," Google in Europe, November 22, 2018.

35 John Frank, "Taking Further Steps to Support Electoral Integrity in Europe," EU Policy Blog, Microsoft, May 3, 2019.

36 "Questions and Answers—General Data Protection Regulation," European Commission, January 24, 2018.

37 "Regulation (EU) 2016/679 of the European Parliament and of the Council," EUR-Lex, April 27, 2016, Art.6(1)(a), Art. 7.

38 Ibid., Art. 15.

39 Ibid., Art. 37-39.

40 Ibid., Art. 83.

41 "First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities," European Data Protection Board, February 26, 2019, 10-11.

42 Nicholas Vinocur, "On GDPR Anniversary, French Privacy Watchdog Says Penalties are Looming", Politico Pro, May 25, 2019.

43 "GDPR Enforcement Tracker."

44 Ibid.

Indeed, smaller entities have struggled to meet the GDPR's requirements while large internet companies have been able to use their dominant position to reinforce their data collection.[45] The latter possess the human resources and in-house expertise to set up the data protection processes required by the GDPR. A sports association in Poland or a local political campaign in Belgium, to take two recent entities sanctioned by DPAs, do not possess the same resources.[46] Yet the GDPR applies uniformly to any entity processing personal data in the EU. In addition, the idea that the consent given to large platforms by their users is informed raises doubts, as users frequently must choose between

> "
> ***The GDPR has invigorated the global conversation around data protection. But the extent to which it should be emulated remains contentious.***

providing their personal data or being unable to use a service they have relied on for years. Lastly, there is evidence that large social media companies have used the legal certainty provided by the "explicit and informed" consent they have collected under the GDPR to venture into even more invasive forms of data collection, with Facebook reintroducing facial recognition in Europe and Google harvesting information on third-party websites.[47]

To its credit, the GDPR has invigorated the global conversation around data protection. A growing number of countries are considering some form of data protection legislation. But the extent to which the GDPR should be emulated remains contentious. In addition to the concerns already highlighted, there is unease around some of the principles in European legislation, most notably the "right to be forgotten," which are open to abuse by authoritarian states.[48] Another objection is that the legislation creates too onerous a burden on European tech companies, and gives an advantage to other states, notably China, where innovation is unimpeded by such laws. For example, developers perfecting the programming of driverless cars and hospitals implementing more effective systems to manage medicine reserves all require crunching vast amounts of data, some of which will inevitably be caught under the GDPR and require its handlers to comply with the law's obligations. To address this risk and ensure that the tech sector can innovate while still respecting privacy, the EU promotes techniques such as anonymization and encryption.[49] It is too early to tell if these mitigation methods will preserve technological innovation in Europe. For now, at the very least, despite the controversies it has generated, the GDPR's enduring appeal shows the ability of democracies to lead the conversation surrounding increasingly indispensable technologies.

5G and Tomorrow's Digital Infrastructure

The evolution of the infrastructure that handles this vast data will be another critical component of European democracies' digitization. 5G technology, the fifth generation of wireless telecommunications, promises to exponentially increase the number of connected devices as well as the amount of information they share. With the increased connectivity expected to carry immense economic benefits, European governments and companies have pushed to get their 5G infrastructure up and running as soon as possible. Many of them have turned to Huawei, the global market-leader on 5G, to help achieve this objective.

Huawei is a telecom giant based in Shenzhen, China and founded by a former officer in the Chinese military. The company's exact ownership is subject to some debate.[50] However, French researchers argue that "its ties with the heart of China's techno-

45 Mark Scott, Laurens Cerulus, and Laura Kayali, "Six Months In, Europe's Privacy Revolution Favors Google, Facebook," Politico, November 23, 2018.

46 "GDPR Enforcement Tracker."

47 Mark Scott, Laurens Cerulus, and Steven Overly, "How Silicon Valley Gamed Europe's Privacy Rules", Politico, May 22, 2019.

48 Owen Bowcott, "'Right To Be Forgotten' Could Threaten Global Free Speech, Say NGOs," The Guardian, September 9, 2018.

49 "Questions and Answers—General Data Protection Regulation," European Commission, January 24, 2018.

50 Christopher Balding and Donald C. Clarke, "Who Owns Huawei?" Social Science Research Network, April 17, 2019.

nationalist project and security apparatus are indelible."[51] In addition, a 2017 Chinese intelligence act compels all Chinese companies "to cooperate with state intelligence and security agencies".[52] Huawei's possible cooperation with the Chinese government has already had direct security implications for Europe. In January 2019, Polish authorities arrested a Huawei employee and a former security official for spying for China. The former official had designed the special phones used by senior officials in Poland.[53]

The United States, Australia and Japan have already banned Huawei equipment from their 5G networks, and the United States has been pushing its European allies to ban the company from building the continent's critical telecommunications infrastructure. In Europe, several intelligence agencies have warned about the national security risks of working with it.[54] Despite this, many European democracies have so far refused to ban Huawei from their 5G infrastructure. To justify this decision, they often argue that the Chinese company is already part of the previous generation of wireless networks and stripping it out before proceeding to build 5G would incur prohibitive costs and delays.[55] In fact, telecommunications equipment is China's largest export to the EU.[56] This reality highlights how dependent Europe already is on technology provided by an entity affiliated with an authoritarian state.

Rather than a ban, Europeans have moved to place strict security conditions on operators that would build their 5G networks. Germany and the United Kingdom are among the countries that have made declarations to that effect. But the question remains very controversial. In the United Kingdom, the leak of one of the National Security Council meetings revealed that ministers were bitterly divided over the decision to allow Huawei to help build parts of the country's 5G telecoms network.[57]

> "*Rather than a ban, Europeans have moved to place strict security conditions on operators that would build their 5G networks.*

The EU has also tried to address the question of 5G. In March 2019, the European Commission issued a series of recommendations pertaining to the cybersecurity of 5G networks.[58] These aim to define certain conditions that providers of 5G infrastructure would have to follow in the EU. The recommendations follow the same approach as that of European states: guidelines rather than bans. Finally, an ad hoc group of EU and NATO members came together in Prague in May 2019 to develop common standards for secure 5G networks.[59]

The number of new interconnected devices that 5G will create dramatically expands the attack surface available to cyber attackers.[60] Allowing companies affiliated with the government of China, a state known to frequently run cyber operations, to build the continent's 5G infrastructure creates unnecessary additional risks and sacrifices the long-term security of Europe's countries for short-term economic considerations.

51 Mathieu Duchâtel and François Godement, "Europe and 5G : The Case of Huawei: Part 2," Institut Montaigne, May 2019.

52 "China's Intelligence Law and the Country's Future Intelligence Competitions," Government of Canada, May 17, 2018.

53 Thomas Morley, "Huawei Espionage Arrests in Poland: A Wake-up Call to Europe," Alliance for Securing Democracy, February 12, 2019.

54 "Huawei 5G in Europe and Beyond," Carnegie Endowment for International Peace, May 2019.

55 Klint Finley, "Huawei Still Has Friends in Europe, Despite US Warnings," Wired, April 25, 2019.

56 "Infographic - The EU and China are Strategic Trading Partners."

57 Dan Sabbagh and Daniel Boffey, "US to Put Pressure on UK Government After Leaked Huawei Decision," The Guardian, April 26, 2019.

58 "Commission Recommendation of 26 March 2019 on Cybersecurity of 5G Networks C(2019) 2335 Final," European Commission, March 26, 2019.

59 "The Prague Proposals: The Chairman Statement on Cyber Security of Communication Networks in a Globally Digitalized World," Prague 5G Security Conference, May 3, 2019.

60 Filip Truta, "5G Will 'Significantly Expand' the IoT Attack Surface, Experts Say," Bitdefender BOX, May 9, 2019.

AI is Already on the Horizon

The development of artificial intelligence (AI) will be a double-edged sword for democracy. It holds the promise of improving human processes and tasks, like detecting deep fakes and other forms of disinformation, but also has the potential for facilitating unprecedented levels of state surveillance. It should be concerning that Chinese entities are pulling ahead of European democracies in the development of effective AI systems, and that authoritarian actors are working together on AI. Megvii, the Chinese company whose facial recognition technology is ubiquitous in the Chinese surveillance apparatus, received financial backing from Russia's sovereign wealth fund.[61]

A January 2018 report by the European Commission stated unambiguously that "Europe is currently lagging behind its competitors in the race for AI leadership."[62] However, EU institutions are beginning to mobilize. In accordance with an AI strategy published in April 2018, the European Commission is increasing annual investments in AI to €1.5 billion for the period of 2018–2020.[63] In addition, the 2021–2027 budget plans to allocate €7.2 billion to AI.[64] Lastly, the EU envisions at least €20 billion of public and private investments in research and innovation in AI through 2030.[65] EU action should also be put in the context of concurrent national efforts. Finland,[66] France,[67] Germany,[68] and the United Kingdom[69] have all put forward AI strategic plans, some of which predated the EU's efforts.

Europeans are also attempting to set standards for the use and development of AI, such as the guidelines for "trustworthy AI" the EU published in April 2019.[70] These guidelines include broad principles like the importance of human oversight, the necessity of building systems that are hard to attack, and non-discrimination, notably in the datasets used to train AI systems.[71] As in the case of the GDPR, the EU's effort has generated debate about the potential pitfalls of over-regulation.[72] Increased cooperation on AI with the United States and other democracies worldwide will work to Europe's benefit. A January 2019 report by a UN agency shows that the United States still holds a significant lead over China in several key dimensions of AI development.[73] Furthermore, the UN report emphasizes that the availability of vast amounts of data in China gives it a de facto edge in the medium to long-term unless "Western nations […] develop better mechanisms to share and pool data."[74]

> *"Europeans are also attempting to set standards for the use and development of AI, such as the guidelines for "trustworthy AI" the EU published in April 2019.*

61 Kai-Fu Lee and Paul Triolo, "China's Artificial Intelligence Revolution: Understanding Beijing's Structural Advantages," Sinovation Ventures and Eurasia Group, December 2017, 12.

62 "USA-China-EU Plans for AI: Where Do We Stand?" Digital Transformation Monitor, European Commission, January 2018.

63 "Artificial Intelligence," European Commission, April 15, 2019.

64 "Member States and Commission to Work Together to Boost Artificial Intelligence 'Made in Europe,'" European Commission, December 7, 2018.

65 Ibid.

66 "Artificial Intelligence Programme," Ministry of Economic Affairs and Employment of Finland.

67 "AI For Humanity: French Strategy for Artificial Intelligence."

68 "The Federal Government's Artificial Intelligence Strategy," Federal Ministry for Economic Affairs and Energy.

69 "Policy Paper: AI Sector Deal," Department for Business, Energy & Industrial Strategy, Department for Digital, Culture, Media & Sport, UK Government, May 21, 2019.

70 High-Level Expert Group on Artificial Intelligence, "Building Trust in Human-Centric AI," Ethics Guidelines for Trustworthy Artificial Intelligence, European Commission, April 2019.

71 High-Level Expert Group on Artificial Intelligence, "Requirements of Trustworthy AI: Diversity, Non-Discrimination and Fairness," Ethics Guidelines for Trustworthy Artificial Intelligence, European Commission, April 2019.

72 Siddharth Venkataramakrishnan, "EU Backs AI Regulation while China and US Favour Technology," Financial Times, April 25, 2019.

73 "Artificial Intelligence," WIPO Technology Trends 2019, World Intellectual Property Organization, 2019.

74 Ibid., 59.

ACKNOWLEDGMENTS

The authors would like to thank President of the German Marshall Fund of the United States (GMF) Karen Donfried, GMF Executive Vice President Derek Chollet, and the GMF Board of Trustees for their support for the Alliance for Securing Democracy (ASD) and commitment to reinforcing the transatlantic partnership.

We are particularly grateful to the many experts in Europe, as well as in the United States and Canada, whom we consulted for input and feedback, including members of ASD's transatlantic Advisory Council. We relied on their experience in and knowledge of Europe's institutions, politics, and society to help shape the analysis and recommendations in this report. We also acknowledge the vast contributions to the literature these experts have made, and on whose reports and commentary we have relied.

Officials and colleagues in various governments and organizations across Europe have graciously shared lessons learned from national efforts to address the challenge of authoritarian interference in their democracies. Many of these best practices from Europe are highlighted in this report, as well as in ASD's initial report from June 2018, the Policy Blueprint for Countering Authoritarian Interference in Democracies, which drew on European lessons learned to make recommendations primarily for an American audience.

We could not have completed this report in a timely manner without the help and dedication of ASD's staff and talented interns, who assisted us in various aspects of this endeavour.

Finally, we thank all Europeans who are working together on the common cause of securing and strengthening democracy against authoritarian attempts to undermine it.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington • Ankara • Belgrade • Berlin
Brussels • Bucharest • Paris • Warsaw

www.gmfus.org