

REPORT

---

# HANDBOOK ON COUNTERING RUSSIAN AND CHINESE INTERFERENCE IN EUROPE



EUROPEAN VALUES  
*Protecting Freedom*



KONRAD  
ADENAUER  
STIFTUNG

2019

---

## EUROPEAN VALUES CENTER FOR SECURITY POLICY

European Values Center for Security Policy is a non-governmental, non-partisan institute defending freedom and sovereignty. We protect liberal democracy, the rule of law, and the transatlantic alliance of the Czech Republic. We help defend Europe especially from the malign influences of Russia, China, and Islamic extremists.

We envision a free, safe, and prosperous Czechia within a vibrant Central Europe that is an integral part of the transatlantic community and is based on a firm alliance with the USA.

Our work is based on individual donors. Use the form at: <http://www.europeanvalues.net/o-nas/support-us/>, or send your donation directly to our transparent account: CZ69 2010 0000 0022 0125 8162.

[www.europeanvalues.net](http://www.europeanvalues.net)

[info@europeanvalues.net](mailto:info@europeanvalues.net)

[www.facebook.com/Evropskehodnoty](https://www.facebook.com/Evropskehodnoty)

---

**This is a joint publication of three European Values programs: Kremlin Watch Program, Red Watch Program and Security Strategies Program.**

### Authors

Martin Svárovský, Head of Security Strategies Program

Jakub Janda, Executive Director of European Values Center for Security Policy

Veronika Víchová, Head of Kremlin Watch Program

Joey Gurney, Intern

Sami Kröger, Intern

### Image Copyright:

President of Russia

This is a joint publication of Konrad-Adenauer-Stiftung and the European Values Center for Security Policy. Konrad-Adenauer-Stiftung assume no responsibility for facts or opinions expressed in this publication or any subsequent use of the information contained therein. Sole responsibility lies on the author of the publication. The processing of the publication was concluded in 2019.

We would like to thank Charles Burton, Senior Fellow at Macdonald Laurier Institute, the team of Sinopsis and several other unnamed specialists for their knowledge sharing and feedback.

---

## INTRODUCTION

European Values Center for Security Policy research team compiled and analyzed European Union, Canadian and US state intelligence reports in order to detect trends among them concerning the threats posed by Russia and China.

The aim of this research was to address the prevailing lack of understanding within the journalism, non-governmental research and policy-making communities on what national intelligence agencies consider to be the main foreign interference threats. While there is a growing amount of existing data on specific foreign interference incidents (particularly with regards to Russian interference in Europe and the US), as well as an increasingly sophisticated understanding and research on the illegitimate tools employed by the Russian and Chinese governments to achieve foreign policy aims, **an in-depth understanding of exactly what those aims are and how they differ across regions and states** is missing. There is also a lack of understanding on how the European and North American intelligence apparatuses have been assessing and responding to these emerging threats. The project therefore aims explicitly to address that gap and thus serve as a tool to further debate on how to respond appropriately and effectively.

The data analyzed in the initial phase of the project covered the period starting from 2013 up to the most recent reports released for the 2018 period, where available. This time frame has been explicitly chosen to evaluate how the threat assessments have changed since the start of the Russian aggression in Eastern Ukraine and the Russian annexation of the Crimean Peninsula.

The outcome of this phase was a published report with the title: *“Russia and China through eyes of NATO and EU intelligence agencies”* report<sup>1</sup>. Key findings of that report included a **clear division inside the EU on how the different member states have reacted into Russia’s and China’s activities in Europe**. The report divided the member states into three categories, the Most Alarmed (Baltic states, Czech Republic, Denmark), the Acknowledgers (Belgium, Croatia, France, Germany, Netherlands, Sweden, UK, US, Canada) and the Hesitants (Austria, Bulgaria, Finland, Ireland, Italy, Portugal, Slovenia, Poland).

The second phase of the project examined Russian and Chinese influence in the Central European region. The aim of the second report was to more closely cover the actual events that have already happened in Central Europe and analyze them as part of the larger picture. The report<sup>2</sup> is divided into two parts: Russia and China. In both cases, the **report goes through the short- and long-term goals for the countries**. These goals have been adjusted to the context of Central Europe: what is the value of Central Europe for Russia and China? How does the region work as a mean towards larger foreign policy goals, and how does the region work as an end itself? After the short- and long-term goals have been listed, the second **report talks about the tools and tactics that Russia and China have used**. The toolboxes have been divided into three categories: economic, political and social tools & tactics. This report also provides key findings about the similarities and differences between Russia and China.

---

<sup>1</sup> <https://www.europeanvalues.net/wp-content/uploads/2019/06/Russia-and-China-through-eyes-of-NATO-and-EU-intelligence-agencies.pdf>

<sup>2</sup> <https://www.europeanvalues.net/wp-content/uploads/2019/12/Analysis-of-Russian-Chinese-Influence-in-Central-Europe-compressed.pdf>

---

## PART 1: WHAT EVERY POLICYMAKER MUST KNOW ABOUT RUSSIAN AND CHINESE INTERFERENCE IN EUROPE

Analysis of the texts of annual intelligence reports has proven what the European Values Center for Security Policy has been claiming for years. The hostile influence operations are not a random occurrence, nor are they a phenomenon that concerns a few countries only. In fact, our research has uncovered a broad consensus among the intelligence agencies in terms of existing tactics and tools applied by Russia and China. In other words, our long-held stance has now been backed by “hard data” i.e. texts of intelligence agencies.

### RUSSIA

*The most prominent threats across the board are the military threat, cyber-attacks and cyber-espionage, media disinformation, economic measures, and increased special services activity in select states.*

#### 1. Ukraine and Russian military threat as an overarching security threat in Eastern Europe.

An overarching security concern of states in groups named “Most Alarmed” and “Acknowledgers” stems from the ongoing Russia-fueled crisis in Ukraine. As mentioned by each of the Baltic states, Russian aggression in Ukraine has set a dangerous precedent for those states that are situated along Russia’s frontier. Not only do Russia’s attempts to publicly justify their strategic campaigns in Ukraine with Russian diaspora cause worry for intelligence officials in the Baltics, but Russian-trained fighters returning from Ukraine to the Baltic states give each of the states cause for serious alarm. **While the Baltic states have demonstrated the most thorough coverage of Russian military exercises and threats along their borders, our analysis has shown that the ongoing conflict in Ukraine has substantially altered the way that Russian military and intelligence threats are assessed**

**by Western European states as well.** Not only does Germany highlight the importance of a democratic resolution to the conflict, but they also reissue how imperative it is for the EU’s solidarity that Russian sanctions remain intact. While intelligence services from the UK, the US and the Netherlands discuss what the resurgence of Russian state based military threats means for overall European security interests, there are also economic effects that the crisis in Ukraine has posed to regions in Europe. Specifically, Croatia highlights how the cold-war style ‘frozen conflict’ in Ukraine has disrupted expected supply routes of Russian oil to the Southeast Balkans. It is clear that Russia’s aggression in Ukraine caused ripples of complications that are felt beyond the realm of military strategy and response, directly effecting the economies of European states who, while remaining aware of the threat from the Kremlin, depend on Russian fuel.

Predictably, the Baltic countries differ in that their reports tend to include realistic and careful appraisals of a direct military threat to their sovereign territory. The Estonian report namely analyzes current threats such as disinformation in the context of how they could be laying ground for Russian success in case of a potential military escalation.

#### 2. Cyber espionage

Several states, including the Czech Republic, Belgium, and Germany, are reporting significant cases of cyber security attacks at the governmental level, and cyber espionage emerged in each report as an essential dimension of the Russian threat. Russian cyber espionage takes on the shape of diffused forms of disinformation attacks, direct interference in governmental servers as well as the slowing down of national IT systems. The Baltic states each observed highly advanced

cyber tools used in espionage campaigns against the processes of state bodies. In the case of Lithuania, 2018 saw an attempted Russian-based cyberattack on their national energy sector. The Netherlands saw similar tactics utilized by Russian intel agencies seeking out information on the Dutch states' scientific programs, economy, defense, and political policies. These digital attacks targeted foreign and defense ministries as well as inter-governmental organizations such as EU, NATO, and the UN, as well as think tanks, NGOs and vital sectors. **A similarity amongst these reports is noting the use of cyber espionage as a military tactic, aimed at destabilizing key national defense options and top-secret intelligence documents.** Named by some as 'active measures' cyber-espionage, especially in Russia's 'near abroad', is mentioned several times as a return to cold-war tactics with an added insidious danger wrought on through the general anonymity of the internet. An overwhelming amount of states have named the Russian cyber threat as a paradigm-shifting phenomenon that the world-at-large needs to combat. This phenomenon pierces through the realm of 'spying' and actually involves attempting recruitment. This new paradigm's difficulty brings with it the problem of differentiating between nationally affiliated cyber actors and independent hackers and cyber-actors. The Baltic states, Netherlands and Sweden have all cited instances of Russian cyber intel initiatives attempting to recruit talented academics, ex-patriots, and military personnel through a variety of online tactics.

### 3. Media disinformation campaigns

Another massive facet of the cyber-threat emerging from Russia is the waging of both publicly executed and privately directed disinformation campaigns. Disinformation campaigns aimed at the curbing of foreign nation's policy and public opinion has been described by the Czech Republic as part of Russia's "hybrid strategy". Germany notes that beyond espionage interests, the Russian services continue to attempt to influence political and public opinion in Germany. Pro-Russian information is spread through social media networks like Twitter, as well as through state-sponsored and private organizations/institutions. Russian state media and their various international affiliates disseminate disinformation about Germany

and attempt to destabilize the German government. Strong hybrid campaigns against Germany's endorsement of EU sanctions against Russia were mounted. The perpetuating of pro-Russian narratives and spreading of seemingly untraceable alternative mainstream discourses have been observed. While some states actually named Sputnik and RT as appendages of the Kremlin's official narrative, the priority of these reports were dealing with how to combat the nefarious spreading of online material that portrays overtly anti-EU, anti-NATO, anti-democratic, anti-pluralistic, and pro-Russian sentiments. **The pro-Russian narrative, as observed by these reports, roughly represent a Euro-skeptical and pro-traditional family value politics that champions the measured conservatism and 'strong-man' politics displayed in Putin's policies.** Estonia, a leader of cyber-security in Europe, observed that by using online news sites, video streaming/sharing sites, and social media, Russia is able to pursue both strategic military and intelligence objectives by harnessing support through the soft effects that disinformation slowly implements. The UK PM also accused Russia of using disinformation to influence the Brexit vote and interfering with UK political party data. Even the United States acknowledged the creation of fake online profiles by Russian accounts to send stolen data to journalists before the 2016 election. Also, the US noted that Russia's state-run media is a propaganda machine that serves as a mouthpiece for the interests of the Kremlin. Canada substantiated these claims in their report, saying that "Russians watch television for an average of four hours a day. Putin and the media emphasize the stability and the greatness of Russia; the state is presented as driving improvements in the lives of the Russian people. The country is portrayed as a fortress and a champion of civilization but is nevertheless surrounded by enemies." Disinformation in the Baltics also takes on the form of the condemning of Russophobia (directed against the Russian minority in the region) and the labelling of Baltic nationalism as overtly anti-Semitic.

### 4. Economic measures

For states with Russian business investment assets, economic risks need to be taken into consideration. The intelligence reports have reflected efforts by both



foreign governments to improve their political and economic standings abroad by carrying out a variety of influence campaigns shrouded by diplomatic cover. The UK namely fears that Russian investments in their critical infrastructure are linked to subversive and criminal finances. For countries with economic dependence on Russian energy, there are instances of reported pressure being applied to support Nord Stream II. **It is fairly evident judging by the reports of France, Germany, Croatia, the Netherlands, and the Baltics, that the consensus among states on what is to be done about Russian aggression varies along economic lines.** For instance, Estonia seems to provide the most positive appraisal of the sanctions, saying their consistency has both surprised Vladimir Putin as well as presented him with substantial and unforeseen domestic problems. Croatia has reached a similar conclusion, stating that they perceive Russia's attempts to thwart other Balkan states from acceding to the EU as economically fueled, and that they have certain dependencies on Russian energy but fear that the current economic climate could lead to Russia acquiring monopolistic gains. The Netherlands pointed out that vital interests of their state have links to private companies with unnamed foreign shareholders, naming this as a threat to their economic well-being. In a similar vein, the Czech Republic has stated its concern that Chinese and Russian career diplomats are attempting to softly coerce Czech officials into fulfilling foreign economic goals. **There are many Russian figures tied up in Czech corruption cases and illegal activities and several Russian investors, stakeholders, and offshore companies involved in the Czech economy.** This situation creates problems for the Czech economy because of some of the key Russian stakeholders' involvement in illegal activities. On the other hand, states like Germany and France take a more conservative approach to how they condemn Russian economic endeavors. Both of them, in a predictably traditional diplomatic manner, claim that combatting Russian aggression economically must not completely ostracize them from the European community, as they are an important economic and political ally.

Direct economic pressure applied by actors of Russian interest also played a paramount role in the assessment of national threats in "Most Alarmed" group. In

Latvia, the issue of investor visas has been contentious, as investor visas are denied to suspected Russian agents. Specific to Denmark is the issue of Arctic sovereignty and maritime demarcation. **The Czech Republic makes it clear that having Russian stakeholders engaged in illegal activities tied up in the Czech private sector makes economic measures regarding Russia an intensely difficult situation.**

### 5. Increased Special Services activity

The Skripal affair greatly affected the United Kingdom's report, and also appeared in several other intelligence reports. There's an ongoing Intelligence committee inquiry into the Skripal poisoning, and the UK's National Security Capability review 2018 remarked that the "reckless and indiscriminate use of a military-grade nerve agent on British soil was an unlawful use of force by the Russian State" (2018, 6). The Belgian report claims that in the wake of the Skripal affair and the Belgian consul being charged with serving the interests of the Russian SVR, Belgian intelligence services have ramped up efforts to root out Russian espionage. Overall, the UK perceives this affair as a reason to put into effect stronger censure policies and more effective counteractive cyber measures against Russia. Meanwhile, the Netherlands' security services have detected increased Russian recruitment efforts with the aim of acquiring political and scientific information, particularly as it pertains to Dutch technological advancements.

**Another secret services tactic that has long been observed is the use of history to spread highly partisan propaganda and amplify societal tensions.** The Russian operation to interfere in the 2016 US Presidential election made heavy use of amplifying racial and class tensions in the US. Narratives which portrayed the US as a surveillance state with excessive police brutality or compared the US to Imperial Rome due to the rising economic inequality and increased concentration of wealth with the so-called "1%" were amplified and supported. **The US example shows Russia taking the tactics that have been at work in Eastern Europe for decades and successfully transferring them to the US context.**

It is evident that the majority of states are highly cognizant of the fact that Russian disinformation campaigns manifest in both the public media sphere (in the form of state and international television, online news sources, etc.) and 'personal' cyber-space (in the form of cyber-espionage, hacking, and spreading of untraceable narratives). Groups "Most Alarmed" and "Acknowledgers" also registered (whether or not they named Russia explicitly) that the global security paradigm has shifted, necessitating the need for intelligence services to ramp up their cyber-defense capabilities. Finally, Russian actors who carry out soft-influence initiatives in foreign states have also been singled out as especially difficult to combat based on the protection afforded to them under the guise of diplomatic procedure.

## CHINA

*Even though Russia featured most heavily in the reports that we compiled, Chinese influence activities were also listed as concerns across all states' intelligence reports, alongside the potential dangers involved in China's growing economic and political ambitions and consequently, power. Some of the trends that we detected include: political and economic pressure applied by China in order to obtain support for their policies (i.e. promoting condemnation of Taiwan and Tibet or territorial disputes in the South China Sea), manipulation of Chinese diaspora for intelligence reasons, and the use of diplomatic covering-up of nefarious operations. China's interests in Europe are also extended and complicated by their alignment with Russia.*

The Netherlands, Denmark and the UK all mentioned concerns about Chinese control and investment in the country's critical infrastructure, which suggests a distinctly different kind of possible economic coercion than the one exhibited by Russia. The Danish report also notes China's economic expansion into the Arctic as a potential future complicating factor, as the region will get linked with other strategic interests. Similarly, Germany has mentioned China's use of political espionage in an effort to gain insights into the workings of the EU or the use of G20 summits.

The Dutch report delves quite substantially into Chinese "profiling" - seeking out individuals for their network of contacts and building long-term relationships. This is not exactly direct recruitment but is nevertheless marked as a concern for the Dutch agency. This mirrors concerns from the Lithuanian report, which notes that China builds relationships with expensive trips, gift giving and so on. An increase of Chinese intelligence activities has also been noted in the Czech Republic.

**The fundamental take-aways from how China was handled in these intelligence reports is that they are a front-runner of international cyber-espionage campaigns and an increasingly relevant player in special services activity in general.** Also, it seems that while China's espionage has traditionally been perceived as economically motivated, this perception is changing as China leverages its economic power and wealth to accomplish foreign policy goals.

While, presently, the Russian threat is both better studied and, at least in Europe, more urgent, a clear conclusion emerges from reading these intelligence reports - that the Chinese threat is serious and will demand an increasing amount of intelligence resources in the coming years. There are notable differences in the Chinese approach in comparison to Russia, particularly as it pertains to economic measures, but there are also worrisome similarities. China's cyber-espionage campaigns have occupied much of the world's attention in the last year. While they have often been different from Russia's in aim as well as

method, both countries have clearly realized the potential of cyberattacks and have the technological means to conduct them. With that in mind, it is safe to assume that more future research will need to be done on the Chinese case. **An understanding of Russian methods and corresponding Western vulnerabilities allows countries to use this understanding as a basis for building more comprehensive security strategies that strengthen resilience against both Russian and Chinese threat.**




## PART 2: COMPARISON OF RUSSIAN AND CHINESE MALIGN INFLUENCE OPERATIONS IN EUROPE

Overall, since roughly early 2018, there has been a major change in modus operandi: **China's embrace of subversive hostile tactics resembles Russia's confrontations with Europe.**

The following table presents a simplified framework for assessing Russian and Chinese strategic influence operations in Europe.

| Simplified comparison of Russian and Chinese influence operations in Europe |   |  |
|---|---|--|
|   | <i>Russian influence operations</i>   | <i>Chinese influence operations</i>  |
| Main strategic objective for the actor                                      | Stay in power as long as possible by limiting the threat of domestic revolution via domination of Eastern Europe and ceasing Western pressure   | Stay in power by externally legitimizing the regime fully controlled by Chinese Communist Party  |
| Ideal end-goal scenario<br>(what is the best-case result)                   | <b>Decouple U.S. &amp; Europe</b> = Europe not a "US proxy territory"<br>Eastern European countries adopt Belarussian governance model (threat of a color revolution diminishes)<br>End of European sanctions against Russia<br>Europe financially sponsors the Russian regime through projects like Nord Stream 2<br>Kremlin oligarchs and their families enjoy life in Western Europe | <b>Decouple U.S. &amp; Europe</b> = U.S. is strategically isolated from its key allies<br>Europe as a legitimization springboard for other regions<br>Europe as market for Chinese tech and business<br>Europe is "neutral" or a potential ally against U.S. on trade issues<br>Europe adopts or tolerates Chinese "globalisation 2.0" |

| <b>Simplified comparison of Russian and Chinese influence operations in Europe</b> |  |  |
|--|--|--|
|  | <i>Russian influence operations</i>  | <i>Chinese influence operations</i>  |
| (Regional) operational objectives of their strategic influence operations          | <p>Germany and France at odds with the U.S.</p> <p>Western Europe effectively tolerates Eastern Europe as a Russian sphere of influence</p> <p>Belt of “neutral” or puppet Central European states (Austria, Slovakia, Hungary, Czech Republic)</p> <p>Poland is strategically isolated</p> <p>U.K. neutralized as resistance actor against Russian aggression</p> <p>German and French political establishment largely strategically co-opted</p> <p>End or regress of EU/NATO “expansion” in Western Balkans</p> | <p>Europe strategically decoupled from U.S. on China-related issues</p> <p>Europe does not counter Chinese influence in Africa</p> <p>Wider Central European and Balkan region (i.e. Greece, Hungary, Serbia) serve as Chinese proxies on selected issues (17+1)</p> <p>European states use Huawei in 5G networks</p> <p>Significant split within Five Eyes</p> <p>Several Western Europe states become Chinese proxies (Portugal, Italy)</p> <p>Europe is intimidated into submission on human rights and Taiwan-related issues</p> |
| Post-2018 modus operandi status  | <p>Russia knows Europe will not effectively punish it for aggressive activities, therefore runs more aggressive influence campaigns</p> <p>Dominant influence over much of European far-right &amp; left</p> <p>Strategic influence successes (Italy, Austria, Hungary)</p> <p>Neutralisation successes (United Kingdom, France, Germany)</p> <p>Mid-term tactical loses (Macedonia, Montenegro, Sweden)</p> <p>Strategic blackmail deals (Nord Stream 2, Paks 2)</p> <p>Decoupling: security vs, trade</p>        | <p>China knows Europe will not effectively punish it for aggressive activities, therefore runs more aggressive influence campaigns</p> <p>China largely achieved political mainstream legitimacy in Europe</p> <p>Chinese aggressive public diplomacy similar to Russia</p> <p>Massive co-optation efforts towards political class, think-tanks and academia</p> <p>Strategic blackmail via interdependence businesses</p> <p>Focus on Huawei &amp; Taiwan issues</p> <p>Decoupling: security vs. trade</p>                          |

A black and white photograph of Xi Jinping, the President of China, standing in front of the Chinese national flag. He is wearing a dark suit, a white shirt, and a patterned tie. The flag features the five-pointed stars and the national emblem. A teal text box is overlaid on the lower part of the image.

There has been a major change in modus operandi: China's embrace of subversive hostile tactics resembles Russia's confrontations with Europe.

---

## KEY SIMILARITIES BETWEEN RUSSIAN AND CHINESE INTERFERENCE MODUS OPERANDI

**SIMILARITY #1: CHINA JOINS RUSSIA IN INTIMIDATION DIPLOMACY TACTICS:** Chinese ambassadors in Europe are more aggressive publicly and privately coerce the hosting states. Chinese diplomacy isn't afraid of "losing face" any more in Europe, since any backlash is not precepted negatively by the domestic audiences due to strong censorship. The Chinese party state has mobilized its resources for aggressive intimidation campaign around two issues: (1) intimidating hosting states into using Huawei technology for the upcoming 5G networks and (2) intimidating hosting states into isolating and de-platforming Taiwan and its representatives from any engagement with representatives of the hosting state.

**SIMILARITY #2: USE OF CORPORATE ECONOMIC INTERDEPENDENCY FOR POLITICAL INTERFERENCE:** China, similarly to Russia, uses reversed economic interdependence. Chinese entities lure major European businesses to China, lets them economically benefit and then coerces them into becoming de-facto proxies of Chinese interference interests. After a while, corporate interdependence is created: specific European businesses want to keep economically benefiting from the Chinese market and therefore lobby their own European governments to be less restrictive towards Chinese interference. Similar trends are visible, for example, within part of the European energy industry when it comes to energy domain.

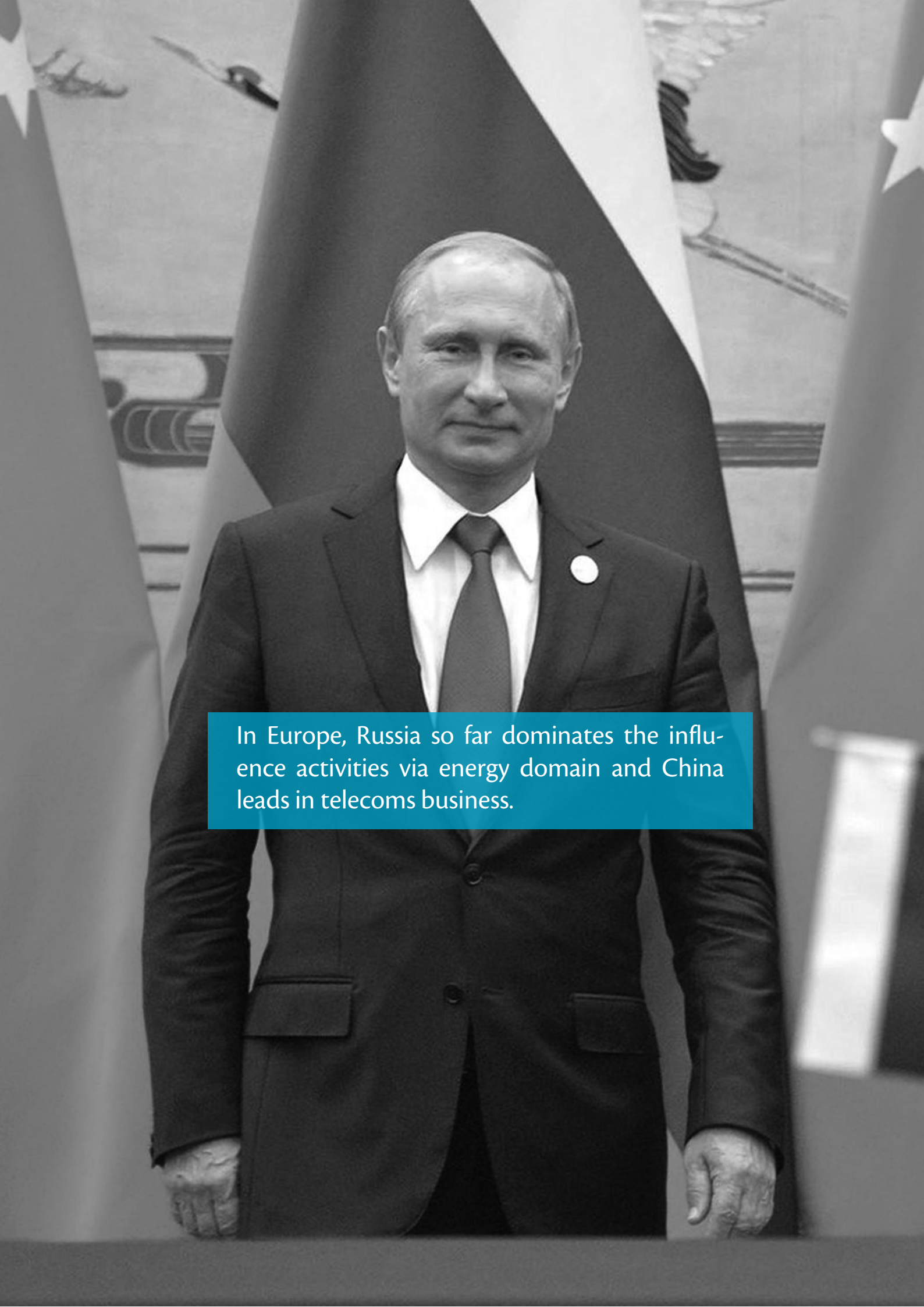
**SIMILARITY #3: "FAKE NEUTRALITY" INTERFERENCE STRATEGY:** Russia has been using the strategic narrative of "fake neutrality" in many countries, mainly in Central and Eastern Europe. The narratives falsely claim that smaller states in the Russian neighborhood can be "neutral", eschewing explicit alignment with either Russia or the EU or NATO, while Russia engages in interference activities in order to achieve elite capture and ideally a state capture situation in the targeted state. A similar strategic influence method is used by China in a slightly different fashion: the pro-Chinese government narratives argue that European states do not have to choose between the USA and China in the US-China confrontation and can "only do business" with China in a way that has no implications for geopolitics and national security issues. The latent anti-Americanism in various Western European countries is a key factor used by Chinese interference entities in these activities.

**SIMILARITY #4: CONVERGING RUSSIAN AND CHINESE INFLUENCE OBJECTIVES IN CENTRAL EUROPE AND WESTERN BALKANS:** While Russia and China are competing for strategic influence in Central Asia, their influence objectives are often converging in Central Europe and the Western Balkans. Russian and Chinese operations often run similar or the same political assets in these two regions, giving the appearance of complementary policies. After all, similar geopolitical objectives in Central Europe and the Western Balkans are shared by Russia and China: to push out the U.S. presence in any form from the region, infiltrate national and local institutions, and ideally acquire elite captures on such a level that Trojan horses scenarios within EU and NATO to the extent that is possible. That is precisely the reason China decided to have the 16+1 (now 17+1 with Greece) format for Central Europe and the Western Balkans. These two regions are institutionally weaker than the rest of Europe and strategic influence over

their elites is possible and the combination of political and economic leverage could neutralize some of the loyal U.S. allies in the 17+1, forwarding one of the key geostrategic goals for China in Europe in the realm of an upcoming U.S. - China confrontation. The division of labor in other strategic sectors seems

to be largely clear: In Europe, Russia so far dominates the influence activities via energy domain and China leads in telecoms business. Strategic competition in these two areas is not visible in these regions and a degree of synchronization can be expected.



A black and white photograph of Vladimir Putin, the President of Russia, standing in front of several Russian flags. He is wearing a dark suit, a white shirt, and a dark tie. A small white circular pin is visible on his left lapel. The background consists of multiple Russian flags, with the white star and blue, white, and red stripes clearly visible. The lighting is even, and the focus is sharp on Putin.

In Europe, Russia so far dominates the influence activities via energy domain and China leads in telecoms business.

---

## KEY DIFFERENCES BETWEEN RUSSIAN AND CHINESE INTERFERENCE MODUS OPERANDI

### DIFFERENCE #1: DISINFORMATION STRATEGIES:

In Europe, Russia organized massive hostile disinformation campaigns which are openly aggressive and focus on (1) undermining citizens' trust in their own democratically elected leaders and (2) attempting to change public views on selected policy issues Russia cares about. Various channels or co-opted politicians, radical leaders, official Kremlin-run communication channels, and domestic proxies are used by the Russian leadership. China does not produce a massive amount of disinformation through many channels in Europe (which is different from Taiwan where communist China does so), but rather uses discourse management to push out issues it doesn't prefer and dominate the discussion through co-opted local leaders and media channels. So far, we have not found dozens of disinformation-producing websites working on behalf of Chinese interests in Europe (which is the usual Russian tactics), since China mainly uses political and media proxies within mainstream discourse to produce its narratives. However, there are examples of the PRC dominating the Chinese-language media space (i.e. in Canada) and it also spreads its information influence via social networks (WeChat).

### DIFFERENCE #2: SCOPE AND FUTURE OF POLITICAL COOPTATION:

While both Russia and China successfully co-opt various European mainstream political leaders and former statesmen, Russia is clearly unable of co-opting massive amounts of young European leaders, while China does it successfully. China has a more long-term strategy and systematically selects hundreds of young future European leaders in various sectors, invites them to mainland China for fully paid and orchestrated visits, and tries to cultivate them while using sophisticated United Front tactics. Russia is capable of similar intensive cultivation efforts mainly on the political and media fringes in Europe, but not among mainstream public institutions on such a massive scale. China systematically builds future networks of political and intelligence assets in Europe. For Russia, strategic corruption projects have been used mainly within the energy domain in Europe.

### DIFFERENCE #3: CHINA CAN SILENCE MUCH OF THE EUROPEAN ACADEMIC COMMUNITY:

While Russia has given up on silencing local critics of the Kremlin in most of European countries, China is systematically trying to co-opt and effectively silence large portions of the European academic community which could be critical of aggressive Chinese policies. The mélange of Chinese-linked funding, programming of Confucius Institutes, activities of Chinese student associations run as part of United Front infrastructures, the serious dependence of some European universities on fees paid by Chinese students, and the intimidation of some European academics by Chinese institutions over visa access all contribute to the fact that, until recently, there was very little in-depth academic research into Chinese interference in Europe.

### DIFFERENCE #4: CHINA DOES NOT SUBSTANTIALLY APPROACH THE FAR-RIGHT: Russia tries

to influence and co-op European far-right political movements and various extremist groups. Until recently, China has largely avoided similar engagement due to potential reputational risks. There are slow changes: In recent years, the Chinese government has successfully engaged with Italian far-right, which facilitated its participation in the formation of the Italian government and its accession to the Chinese-led Belt and Road Initiative. There are signs that in the future, China might turn to the strategy of cultivating the far-right more and more, as we can see similar efforts i.e. in Sweden, but still not comparably to the scope of the Russian tactics.

## PART 3: FRAMEWORK POLICY STRATEGY FOR RESPONDING TO CHINESE INTERFERENCE

We divide the policy responses into four key areas:

### Response area #1: DOCUMENTING AND INCREASING UNDERSTANDING OF THE THREAT

**Measure #1: Public documentation of the hostilities.** Non-governmental organizations and experts have responsibly and diligently documented and informed the public on the incidents and modus operandi of the PRC's hostile influence. They must use their connections to journalists, public officials, and the wider public and provide an information service about the state of play.

**Measure #2: Exposing the nature of the PRC's totalitarian regime.** Non-governmental organizations, experts, and journalists should raise the public awareness of the aggressiveness of the PRC toward its own population and the totalitarian nature of its communist regime.

**Measure #3: Parliamentary investigations of the influence networks.** All EU Member States should launch their own parliamentary investigations of PRC's influence networks in their respective countries, similarly to how the US and the UK conducted parliamentary inquiries into the Kremlin's influence and disinformation. Such processes open the public discussion about the threat, expose new details, and elucidate the complex picture of the public discussion about the threat can emerge.

**Measure #4: The national security and intelligence establishments should publicly call out the threat** of the influence of the PRC. Even though national security and intelligence institutions cannot and should not conduct public inquiries, they can openly describe the character and the scope of the PRC's hostile influence in some of their public outputs, i.e. in their annual reports, similar to how the intelligence ser-

vices of the Baltic countries highlight the most important incidents of the Kremlin's influence.

### Response area #2: MOBILIZATION OF OUR SELF-DEFENSE

**Measure #5: The main governmental driver.** Every country should establish a government entity that cooperates closely with the intelligence community but is itself independent, so that it can develop and drive policy and operational activities.

**Measure #6: Funding and protection for domestic researchers.** To support the network of independent experts who need security and freedom to study and inform about the PRC publicly, the government has to provide sufficient funding and protection for such organizations and individuals. This way it can avoid most of the national experts on China being blackmailed or directly funded by the PRC.

**Measure #7: National strategy on China.** All EU Member States should design a national strategy document on how to handle relations with the PRC in the future, which would include the main priorities vis-à-vis China, the types of threats and challenges originating in the relationship, and what goals the country wants to fulfil vis-à-vis the PRC.

**Measure #8: Incorporation of the PRC's influence into the counter-influence agenda.** The PRC's hostile influence should be incorporated into the counter-influence agenda of the already existing teams focusing on the hostile influence of the Kremlin (i.e. Center against Terrorism and Hybrid Threats in the Czech Republic, the Civil Contingencies Agency in Sweden, etc.) Those units should hire experts on China and combine their knowledge instead of establishing new separate institutions.

**Measure #9: Exposure of the PRC's disregard for**



**human rights.** The governments of the EU Member States should publicly expose and call out the track record of the PRC in breaching human rights, as well as acknowledge all individual incidents. This approach of the PRC should always be taken into account when dealing with public officials of the PRC.

**Measure #10: Briefings for NGOs and journalists.**

Governments of the EU Member States should offer expert non-classified briefings for representatives of the non-governmental sector and journalists. These briefings can be used to inform the target audience about the threat assessment of PRC's influence and explanation of the country's approach towards PRC, but also to inform and warn the target audience about what can be expected when engaging with the PRC.

**Response area #3: DETERRENCE AND PUNISHMENT (RAISING COSTS) OF THE AGGRESSOR AND ITS PROXIES**

**Measure #11: Transparency in academia.** Governments and the non-governmental organizations should work on improvement of the transparency of the hostile influence of the PRC in the academic sector. It cannot and should not be forbidden for individual academics, universities and academic institutions to travel to the PRC or to accept financing from the Chinese government; those decisions are in the hands of the universities themselves. However, those activities should be acknowledged and transparent for the public.

**Measure #12: Every Western country should adopt its version of the Magnitsky Act and Mechanism for Screening of Risky Foreign Investments.** Democracies have a clear right to defend human rights and their own sovereignty. Therefore, every Western democracy should implement its own version of the Magnitsky Act and Mechanism for Screening of Risky Foreign Investments.

**Measure #13: Transparency of foreign lobbying.**

National governments and parliaments should introduce and abide by rules for transparency of foreign lobbying, similarly to the already existing FARA in the US or the Transparency Scheme in Australia.

**Measure #14: Protection of state cyber infrastructure.**

Governments and parliaments should acknowledge the recommendations of the cyber-experts and state cyber agencies and protect the state cyber infrastructure against PRC technology. Such technologies can be banned from participating in state infrastructure projects if necessary.

**Response area #4: IDENTIFICATION OF OUR WEAKNESS AND RESILIENCE BUILDING**

**Measure #15: Standards for civil servants when engaging with the PRC.**

Governments should establish and abide by basic standards for civil servants in situations when they are engaging with the PRC and its officials. The governments should ensure that they are sufficiently informed about what challenges and threats that might be posed and how to handle such situations without being vulnerable.

**Measure #16: Standards and consultations with national and local businesses.**

Governments should establish basic (voluntary) standards and provide consultations and advice to national and local business which are working with or in the PRC or are considering doing so. Companies like that should be provided the basic threat assessment and a set of recommendations on how to engage with the PRC.

**Measure #17: Governmental expertise.**

Governments should increase their in-house expertise on the PRC by hiring established experts on the issues of the PRC, especially in connection to the security field.

**Measure #18: Scenario-building.**

Western governments should engage in scenario-building of potential development of the PRC's influence in their respective countries. That can be done by analysing the influence strategies of the PRC in other countries and projecting this information into the local situation.



## PART 4: FRAMEWORK POLICY STRATEGY FOR RESPONDING TO RUSSIAN INTERFERENCE

This policy framework is part of the Kremlin Watch Strategy published by the European Values Center for Security Policy in December 2019.<sup>3</sup> The following text is a summary of the Strategy.

### Proposed measures:

#### Response area #1: DOCUMENTING AND INCREASING THE GENERAL UNDERSTANDING OF THE THREAT

**Measure #1: The main governmental driver.** Every EU Member State should establish a government entity that cooperates closely with the intelligence community but is itself independent, so that it can develop and drive policy and operational activities.

**Measure #2: “A European StopFake”:** Every country and the EU as a body need to have daily situational awareness and myth-busting capability with practical countering of disinformation incidents. The EEAS East STRATCOM Task Force has developed a wide network of experts from Georgia to Belgium as part of its weekly Disinformation Review. The national governments should make sure that this already existing and proven network, including a solid analytical team at the EEAS East STRATCOM Task Force, is appropriately funded and delivers analysis and counters Russian propaganda narratives daily.

**Measure #3: The underfunded EEAS East STRATCOM Task Force should become the EU’s main analytical and response body.** While Federica Mogherini has sabotaged this team,<sup>4</sup> it is clear that the next High Representative must make this, the *only* EU-wide and European Council-mandated body, the real headquarters of the EU response to Russian disinformation. The EU Member states should make sure that the EEAS triples the personal capacity of the team and that at least 5 million EUR annually<sup>5</sup> are used for countering Russian disinformation, not general PR for the EU.

**Measure #4: Regular polling and in-depth sociological research to evaluate the scope of the problem:** Every Member State should conduct regular polling and sociological research to measure public support for the most common Russian disinformation narratives. In practice, the top 10 Russian disinformation narratives should be tested among the portions of the target population that are expected to believe them; follow-up sociological research, e.g., focus groups, should aim to explain the reasons behind the success of specific disinformation narratives. This exercise should be conducted every six months, so that the progress of both the threat and the tailored counter-measures can be regularly evaluated.

<sup>3</sup> <https://www.europeanvalues.net/wp-content/uploads/2019/12/Kremlin-Watch-Strategy.pdf>

<sup>4</sup> POLITICO: Federica Mogherini ‘soft’ on disinformation, critics say, 22.3.2017, WWW:

<https://www.politico.eu/article/vladimir-putin-opponents-pile-onto-federica-mogherini-eaststratcom-sandra-kaliete-jakub-janda-estonia-atlantic-council-ben-nimmo-fake-news-russia-putin-europe-foreign-policy/>

<sup>5</sup> European Values Think-Tank, Open Letter by European Security Experts to President of the European Commission J. C. Juncker and High Representative for Foreign and Security Policy Federica Mogherini, WWW:

[https://www.europeanvalues.net/openletter/?utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=kremlin\\_watch\\_briefing\\_the\\_eu\\_has\\_to\\_start\\_taking\\_pro\\_kremlin\\_disinformation\\_seriously&utm\\_term=2019-03-24](https://www.europeanvalues.net/openletter/?utm_source=newsletter&utm_medium=email&utm_campaign=kremlin_watch_briefing_the_eu_has_to_start_taking_pro_kremlin_disinformation_seriously&utm_term=2019-03-24)

**Measure #5: All EU Member states should launch their own parliamentary investigations of Russian influence networks in their respective countries.**

The US and UK parliamentary inquiries have shown why such a process is needed – it opens the public discussion about the threat, new details and the complex picture of the situation emerges, if done correctly, and the national security institutions are required to explain the nature of the threat in an adequate parliamentary setting. The intelligence community should never be asked to conduct a public inquiry (even with sensitive details classified), and neither journalists nor experts could ever see the whole picture. Therefore, it should be led by parliaments with the power to constitutionally check the executive branches and their readiness to defend national security.

**Measure #6: National intelligence agencies in EU states should be as transparent as their Baltic counterparts.** Naturally, no intelligence agency will ever willingly disclose its methods or sources. Nevertheless, the Baltic intelligence communities are leading the way among allies in publishing detailed annual reports and making arrests of Russian operatives as public as possible to show their society what the threat looks like. Many other European agencies are slowly following this trend.

**Response area #2: MOBILISATION OF OUR SELF-DEFENCE**

**Measure #7: Every country should appoint an Ambassador-level Special Envoy for this agenda.** Because this issue crosses several policy fields, and debates between allies are highly intensive, every country should have a go-to representative who serves as a spokesperson for their country's approaches and plays a domestic role for the government's voice on this issue. Baltic and Scandinavian states have already appointed similar Special Envoys; other allies should do so as well.

**Measure #8: The new Council disinformation working group (ERCHT) should be used for practical steps.** This new specialized working group at the Council of the EU is currently dedicated only to the disinformation agenda but should be used for creat-

ing regular joint threat assessment and sharing practical case studies and best practices. Additionally, EU institutions need to receive regular briefings and guidelines from national specialists, which is currently not happening on enough scale.

**Measure #9: All EU Member states should set up regular funding mechanisms for their respective civil societies regarding this issue.** Currently only a minority of EU Member states fund civil society initiatives to counter this threat. Nevertheless, much of the political rhetoric in Europe is led by rhetoric about "civil society-driven response". Ironically, within this field the EU often provides much more funding for activities outside of the EU than it does for work within the EU. This is based on the belief that EU Member states are responsible for their own domestic situations. Nevertheless, due to political sensitivities and often a lack of political will, real funding for civil society to counter this threat is almost non-existent. Even though it is possible for NGOs to get funding for research or media literacy issues, it is significantly harder to secure funding for myth-busting, accountability, or security activities. Every EU Member State should set up a funding mechanism, possibly in cooperation with its like-minded allies or the private sector, to practically support the capacity-building of its own civil society. For example, many Western European countries clearly lack the expertise on Russian matters. The role models for such specialised centres are the Centre for Polish-Russian Dialogue and Understanding (CPRDIP), the Estonian Center of Eastern Partnership, or the Polish Centre for Eastern Studies (OSW).

**Measure #10: Every EU member state should support the establishment of groups like the Baltic Elves.** Citizen-led bottom-up initiatives for myth-busting and countering extremist tendencies in society are a key response to this threat. Governments should not run or organise its civil society, but there are ways in which they can incentivise and support similar projects – from providing funding for capacity building and training to protecting its own citizens from foreign or extremist harassment. Proven concepts such as community policing and crowd-sourced social work are relevant examples from other policy areas.

### **Response area #3: DETERRENCE AND PUSHBACK AGAINST THE AGGRESSOR AND ITS PROXIES**

**Measure #11: European allies should significantly harden their approach to personal and financial sanctions against Russian hostilities.** Firstly, European countries should level their sanction-related actions with the US. For example, it is a sad indicator of European weakness that one of the key Kremlin proxies in Europe, Vladimir Yakunin, is only on the American, and not EU, sanction list. Leaders of Russian disinformation efforts should be personally sanctioned, so that each of them understands that conducting hostilities against European democracies has personal consequences. Many Russian “NGOs”, “private foundations”, “private enterprises”, and “media” are either state-owned, have hidden ties through complex schemes, or depend on state funds, the cooperation of the Russian state, or Putin’s personal entourage for their activities, and so report to the Russian state and state agencies and must adjust their policies accordingly. There are very few organisations that stay clear of Russian governmental interference (like Memorial), and Western states need to draw a distinction between the two when they talk about “dialogue” with “civil society”, since MGIMO, as an example, or various Kremlin-linked think-tanks effectively do not represent civil society, but rather the Russian regime and its intelligence community.

**Measure #12: Western allies should escalate their**

**pushback, including sanctions, until Russia ceases hostilities.** Western allies should draft a joint list of Russian oligarchs connected to the Kremlin (such as the one the U.S. has) and announce that, until Russia stops specific hostilities (for example, until it releases Ukrainian sailors and other Ukrainian political prisoners), they will escalate the sanctions by a certain percentage every week. Such pin-pointed economic action would bring the initiative to the Western side in demanding action and pushing the Russian government with legitimate and clearly defined end-goals. Similarly, all relevant family members of leaders of Kremlin-linked organisations living in the West should be put on a list, and if Russia does not cease hostilities, legal ways should be found for them to be sent back to Russia. Western democracies have legitimate reasons to attack the Kremlin’s weak points to make it cease hostilities, ranging from the killings and occupation in Ukraine to hostile interference activities in the West.

**Measure #13: Western governments should make the fortune of Vladimir Putin and his associates public.** It is clear that the regime led by Vladimir Putin has been stealing from the Russian state on a large scale in sharp contrast to the transparency of liberal democracies. Therefore, Western institutions should make sure that it is publicly known how much and in what ways Vladimir Putin, along with his associates and shadow supporters, has stolen from Russia. A bill with this goal is currently being discussed in the US Congress.<sup>6</sup> It can take the form of official records or be distributed to the press, who would verify and make it public. The objective of this tool is to make sure that the Kremlin elite understands that it is going down a one-way street and it (or its families and proxies) will never be able to enjoy its stolen money for a comfortable life in the West.

**Measure #14: Like-minded European countries should prepare massive expulsions of Russian intelligence officers.** Many European countries face disproportionately large Russian diplomatic missions where between one third and one half of the members conduct hostile intelligence tasks. Since even President Putin calls for “diplomatic parity”, like-

<sup>6</sup> The U. S. Congress, H.R.1404 - Vladimir Putin Transparency Act, WWW: <https://www.congress.gov/bill/116th-congress/house-bill/1404?q=%7B%22search%22%3A%5B%22putin%22%5D%7D&s=2&r=1>

mind countries should prepare for joint action, so that once they decide to go ahead (for example, after another Russian hostility), they can expel large numbers of Russian intelligence officers to “clean house.” Russia will retaliate by sending European diplomats home, but if it is done in collective action by at least 5-7 EU countries, it will be difficult for Russia to severely punish only one Member State. Therefore, the expected outcome will be the annulling of a number of Russian diplomats in the targeted European countries and vice versa, which will lead to a fresh start after a couple of months – EU countries will start proportionally staffing their embassies one by one – in parity with Russia. The goal for European countries is to achieve a de-facto disbanding of the majority of Russian intelligence networks in their countries. However, it is neither practical nor desirable to band all Russian intelligence networks; those which function as part of the SVR’s “illegals” programme, for example, are often highly integrated into their target countries.

**Measure #15: Every European country should have its own Mueller-style in-depth investigation into Russian interference incidents.** It is important that parliaments publicly investigate the scope of the Russian influence threat using an in-depth special inquiry similar to the one the US Department of Justice has launched after Russian interference in 2016 US presidential elections. Often law-enforcement is not skilled or equipped to inquire on specific incidents related to complex Russian interference operations. Therefore, a team of specialists from law-enforcement or counter-intelligence should be assembled to investigate specific recent cases of Russian offline and online influence operations, for instance, in Russian influence operations related to Nord Stream 2, the Dutch 2016 EU-Ukraine Association Agreement Referendum, and the 2017 French presidential elections.

**Measure #16: All European countries should stop legitimising Russian disinformation tools posing as “journalistic platforms.”** Communication channels effectively run by the Russian government, be it RT, Sputnik, or Russian state-run TV channels, masquerade as journalism. Therefore, European countries

should not consider them to represent free media, and rather ban them from press conferences and deny access that is granted only to journalists, which they are not. This would send a clear message that working for the Russian government is a one-way street for any so-called journalist. No Western public official should ever legitimize these entities with an interview.<sup>7</sup>

**Measure #17: Every parliament should exercise their ethical standards, including against those parliamentary Members serving Russia and Russian interests, and not their constituents or allies.**

While parliamentarians are free to express any opinion, they must be under scrutiny by their peers if their loyalty towards Russia’s aggressive foreign policy interests exceeds their loyalty to the institution they have sworn to represent. For example, if somebody acts as a Kremlin proxy in the security committee or travels to legitimize Russian occupation of Ukrainian land in Crimea, such a parliamentarian should be subject to a public hearing and potentially expelled from specific committees or bodies of the parliament.

**Measure #18: Every Western country should adopt its version of the Magnitsky Act and Mechanism for Screening of Risky Foreign Investments.** Democracies have a clear right to defend human rights and their own sovereignty. Therefore, every Western democracy should implement its own version of the Magnitsky Act and Mechanism for Screening of Risky Foreign Investments. Western governments should stop ignoring the threat posed by dirty Russian money.

<sup>7</sup> Example: then-German Foreign Minister Sigmar Gabriel providing RT with an exclusive interview: <https://www.youtube.com/watch?v=sBtNQaaahX4>

#### Response area #4: IDENTIFICATION OF OUR WEAKNESSES AND RESILIENCE BUILDING

**Measure #19: Western governments must put principled pressure (including hard regulation) on tech-giants enabling and benefiting from the massive spread of disinformation.** While Russia is the main source of hostile disinformation, platforms like Facebook, Twitter, and Google are the principal enablers of this phenomenon hostile to liberal democracies. Every EU Member State should appoint a national coordinator for policies regarding tech platforms and every Member State should adopt a comprehensive strategy that aims to mitigate the spread of disinformation and protect personal data.

**Measure #20: Western governments must fund effective and systematic digital and media literacy programs.** Most Western governments are failing to deliver modern civic education to its citizens on issues surrounding the information environment. Large but effective programs should be part of a well-thought-out national strategy helping citizens understand the rapidly changing information environment.



