



Clingendael

Netherlands Institute of International Relations

SEPTEMBER 2018

Hybrid Conflict and the Future European Security Environment

Russia remains the most active and aggressive hybrid threat actor confronting Europe. Information Confrontation, including targeted disinformation and propaganda, remains the central element of Russia's hybrid activities, enabled by sophisticated cyber operations. Over the past year, Moscow has demonstrated a growing willingness to employ high-risk and even lethal hybrid actions, to include the use of an advanced chemical nerve agent on European soil. A heavy Russian hybrid focus on its so-called 'near abroad' is likely in the near future. Moreover, Russia will almost certainly employ hybrid tools against Western Balkan states, especially the Former Yugoslav Republic of Macedonia, in a targeted effort to discourage or delay its accession into the Euro-Atlantic institutions. China's hybrid activities, on the other hand, are more discreet and mostly emphasize technology theft and intelligence gathering. However, China's growing economic presence in Europe and its desire to shape international norms creates the potential for Beijing to become a much more significant hybrid challenge over the long term. It is anticipated that the Democratic People's Republic of Korea will continue to pose only a limited hybrid threat against Europe.

Strategic Alert

Danny Pronk

Russia Remains the Principal Hybrid Threat Actor Against Europe

Over the past year, Russia has once again demonstrated both the capability and intent to employ a wide range of hybrid tools to undermine European interests. Russian actors have sustained ambitious disinformation campaigns, conducted

cyber-attacks, targeted critical (election) infrastructure, fueled social discord through the use of proxies, and almost certainly used chemical weapons on European soil. These actions are intended to undermine the foundation of Europe, erode confidence in the media, silence the Kremlin's critics, and interfere in the democratic processes of European countries. These geopolitical goals shape Russia's hybrid campaign against both Europe. In particular, President Putin

Strategic Alert

seeks to prevent an expansion of European influence in its so-called 'near abroad'. The Kremlin fears a continued erosion of its traditional sphere of influence, continuing from the Baltic States to the Western Balkans. Although other states, including China and the Democratic People's Republic of Korea possess hybrid capabilities, no state actor currently comes close to rivalling Russia's ambitious hybrid campaign against Europe.¹

Russia's Main Hybrid Weapon Against Europe is Information Confrontation

Russia utilizes Information Confrontation as the predominant form of hybrid activity against Europe, as it seeks to dominate the information sphere.² Russia's widespread disinformation and propaganda campaigns rely heavily on traditional media platforms (i.e. radio, television), amplified with internet-based media, including websites, blogs, and social media. These campaigns target both domestic and foreign audiences.³ Information Confrontation activities are assessed to be sustained by the Saint Petersburg-based Internet Research Agency and similar organizations. Pro-Russian narratives are frequently amplified online by a network

of trolls and automated language bots, particularly on *Twitter* and *Facebook*. These tactics are used to foment political, social, ethnic, or racial divisions in the targeted population. The challenge posed by Russian Information Confrontation is growing. Over the past year, Russian state-sponsored media outlets have expanded their presence throughout Europe and beyond. *Russia Today* now broadcasts in Russian, English, Arabic, Spanish, and French, and has announced plans to create a German-language outlet in the future. A similar trend is evident in the Western Hemisphere, with Information Confrontation efforts focused against the U.S. in particular. Russia has also been promoting its Spanish-language media outlets to the Latin American audience.

Russia's Cyber Capabilities Greatly Enhance its Information Confrontation Efforts

Russia relies on cyber activities to enable Information Confrontation efforts, particularly by accessing sensitive or damaging information on opponents. Once such information is obtained, various media tools and botnets are employed to reach a wide audience. In recent years, Russian actors have also used cyber tools to infiltrate networks controlling critical infrastructure, such as electrical power grids. Russian-linked Advanced Persistent Threat (APT) networks were highly active over the last year. Numerous APTs, including the Russian military intelligence (GRU)-linked APT 28 were deeply involved in conducting cyber intrusions and attacks against EU member states, civil service, military (especially defense industry) and academic institutions, and critical infrastructure.⁴ Russian state and state-sponsored cyber actors likely attempt to conduct cyber intrusions on a daily basis in order to gain the advantage on the Information Confrontation battlefield.

1 For a more in-depth look at hybrid conflict and the roles of Russia, China, and the Democratic People's Republic of Korea, see: Van der Putten, Frans Paul, Minke Meijnders, Sico van der Meer and Tony van der Togt, eds. *Hybrid Conflict. The Roles of Russia, North Korea and China*. The Hague: Clingendael Institute, 2018.

2 'Information Confrontation' is a broad term that includes military and non-military information campaigns, psychological operations, propaganda, strategic denial and deception, and electronic warfare, as well as cyber-attacks and other technical operations. These activities are conducted in order to influence an opponent's key institutions, leadership, public opinion, armed forces, etc. Althuis, Jente and Leonie Haiden, eds. *Fake News. A Roadmap*. Riga: StratCom CoE, 2018. p. 60-62.

3 Van der Putten, Frans Paul, Minke Meijnders, Sico van der Meer and Tony van der Togt, eds. *Hybrid Conflict. The Roles of Russia, North Korea and China*. The Hague: Clingendael Institute, 2018, p. 8-13.

4 APT 28 is considered to be one of the most prominent and aggressive Russian cyber threat actors, and to have conducted large scale cyber operations to interfere with several recent elections in both Europe and the U.S.

Strategic Alert

Cyber capabilities will remain an essential aspect of Russia's hybrid campaign, especially as cyber activities are difficult to attribute and have the capability to effectively erode European cohesion.

Russian Intelligence and Security Services Play an Integral Role in Hybrid Operations

Operatives of the Russian Intelligence and Security Services, in particular GRU military intelligence, play a key role in a variety of direct and indirect actions against Europe.⁵ Whenever Russia's interests are at stake, or if the Kremlin believes specific actions are essential to achieve certain goals, it is highly likely that the Intelligence and Security Services will be involved, often to provide oversight and initiate so-called 'active measures' to ensure that Moscow's interests are protected and its goals are attained.⁶ The Intelligence and Security Services embed operatives in civil society engagement organizations, and seek to infiltrate foreign national institutions, law enforcement, political parties, and NGOs, to gather information and influence decision-making processes.⁷ Within a hybrid context, the Intelligence and Security Services play an important role in identifying fissures in target countries, and then developing plans and employing resources to more effectively exploit these fissures. Due to the discretion employed, individuals and organizations can play unwitting roles in such operations, and identification and attribution of Russian involvement in certain actions remains difficult.⁸

5 <https://www.theguardian.com/world/2018/aug/06/the-gru-the-russian-intelligence-agency-behind-the-headlines>; <https://spectator.clingendael.org/nl/publicatie/inlichtingendienst-groe-de-schaduw-van-de-kgb>

6 <https://www.hybridcoe.fi/wp-content/uploads/2018/05/Strategic-Analysis-2018-4-Juurvee.pdf>

7 <https://www.lawfareblog.com/document-indictment-against-mariia-butina>

8 <https://www.hybridcoe.fi/wp-content/uploads/2018/06/Strategic-Analysis-2018-5-Cullen.pdf>

Russian Military Posturing Plays a Key Role in Russian Information Confrontation

Although Russian military exercises, such as VOSTOK 2018 (the most recent iteration of a major Russian exercise that occurs every year), serve primarily to develop Russian military capability, they also play a key role in demonstrating Russia's great power status and readiness to the world. Military exercises and other displays of military prowess, such as Russia's current military operations in Syria, support the strategic messaging for Russia's Information Confrontation efforts. Over the past year, Russia has also demonstrated a willingness to develop and sponsor paramilitary organizations that further Russian interests. This trend has increased since the 2014 Ukraine crisis, where Russia used numerous paramilitary organizations to fight in the Donbass. Russia has also used Private Military Companies (PMCs), especially the *Wagner Group*, in Syria, Central Africa and the Western Balkans. The facilitation and sponsorship of Russian PMCs and other paramilitary groups has enabled Moscow to utilize a cadre of skilled paramilitary operatives in a variety of non-attributable hybrid actions wherever and whenever required by the Kremlin.⁹

Russia Focuses its Hybrid Activities on its So-Called 'Near Abroad'

Russia devotes a significant level of its hybrid activities towards its so-called 'near abroad', with an aim to prevent states within these regions from abandoning the Russian sphere of influence in favor of the Euro-Atlantic

9 <https://www.lawfareblog.com/semi-state-security-actors-and-russian-aggression>; <https://jamestown.org/program/beyond-syria-and-ukraine-wagner-pmc-expands-its-operations-to-africa/>; <https://foreignpolicy.com/2018/08/08/putin-is-building-a-bosnian-paramilitary-force/>

Strategic Alert

institutions.¹⁰ This is particularly true in states that have exhibited an inclination of joining NATO and/or the EU, like Ukraine, Moldova, and Georgia, and the Western Balkan states of Serbia, Bosnia and Herzegovina, and, more recently, the Former Yugoslav Republic of Macedonia. Moscow is using pro-Russian movements, personal and business connections, as well as corruption and organized crime to pursue its interests in these regions. As it moves closer to NATO and the EU, the Former Yugoslav Republic of Macedonia is very likely to face intense Russian hybrid activity. In March 2018, Russia's ambassador to the Former Yugoslav Republic of Macedonia ominously warned Skopje that it would become a "legitimate target" if it continued down the path of accession.¹¹

Russian Civil Society Engagement Continues to Build Support Outside of Russia

Moscow has strengthened its civil society engagement programs, utilizing a range of government-organized NGOs (GONGOs), proxy NGOs, and other state-sponsored organizations to shape public opinion and advance its interests.¹² This engagement

includes establishing cultural centers in key cities and regions that focus in particular on building connections with potentially sympathetic Russian compatriots. Moscow also employs think-tanks to create pro-Russian domestic and international narratives, often providing the false impression of an objective, academic voice, and it identifies and supports opinion leaders who can advance Russian narratives, leverage organized crime networks, and manipulate Orthodox-Slavic Christianity and identity through the influential Russian Orthodox Church. Moreover, Russia's engagement includes sponsorship of multiple ultranationalist groups that seek to advance Russian interests throughout Europe. One of the most prevalent examples is the *Night Wolves* motorcycle club, an ultranationalist movement that has chapters throughout Eastern Europe.¹³

Russian Employs Economic/Energy Leverage in its Neighborhood and Against Europe

Although Russia's overall economic power is currently limited, it has the ability to employ energy leverage in its direct neighborhood and against EU member states. Russia uses its dominance in the energy field as an instrument of economic, political, and diplomatic influence and coercion, as well as a tool of corruption. Moscow will likely seek to expand its presence in the European energy market in order to generate revenue and access strategic infrastructure and assets in EU member states. This includes the construction of new gas pipelines to Europe (i.e. Nord Stream 2 and Turk Stream). In addition to generating revenue for Russian exporters, the construction of new export gas pipelines will considerably erode the importance of current export routes through Belarus and Poland, as well as through Ukraine, Slovakia and Czech

10 The concept of the so-called 'near-abroad' is debatable, as this could encompass not only the states within the 'post-Soviet space' (the former Soviet states of Belarus, Moldova, Ukraine, Georgia, Armenia, Azerbaijan, Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan, Uzbekistan, Estonia, Latvia, and Lithuania), but also former Soviet-dominated territories in Eastern Europe, such as Poland, Czech Republic, Slovakia, Hungary, Romania, and Bulgaria, and possibly even the Western Balkan states of Serbia, Montenegro, Slovenia, Croatia, Bosnia and Herzegovina and the Former Yugoslav Republic of Macedonia.

11 https://www.ecfr.eu/publications/summary/do_the_western_balkans_face_a_coming_russian_storm

12 Van der Putten, Frans Paul, Minke Meijnders, Sico van der Meer and Tony van der Togt, eds. *Hybrid Conflict. The Roles of Russia, North Korea and China*. The Hague: Clingendael Institute, 2018, p. 5-7.

13 Gobert, Sébastien, 'The Night Wolves Settle in Slovakia, and the Kremlin With Them?', *RUSI Newsbrief*, 16 August 2018.

Strategic Alert

Republic. Diverting export to new routes likely will increase economic pressures on those countries, as Russia could use tactics such as the disruption of gas deliveries and price manipulation to achieve its geopolitical goals. Several European countries remain highly vulnerable to energy leverage and pressure. In order to retain and secure this, Russia will likely further utilize hybrid tools, including Information Confrontation, hostile lobbying, informal business channels, and intelligence activities.

China Has the Potential to Become a Highly Significant Hybrid Threat Actor Over the Long Term

Although Russia remains the most active and aggressive hybrid threat against Europe, China also has the resources and tools to advance its interests through hybrid means. China's expanding global power and influence has implications for all European states and could eventually challenge interests on a significant scale. In terms of strategic goals, Beijing seeks to ensure the continuity of economic growth, advance its geopolitical influence, assert Chinese security interests, and sustain single-party rule. Hybrid activity is an important tool to support these objectives. China's employment of hybrid tactics still remains most visible and successful in East Asia, particularly in dealing with less powerful states. Through a calculated approach, over the course of the past decade Beijing has dramatically expanded its military and civilian presence in several disputed areas in the South China Sea, without triggering a military reaction. Although China currently is more cautious in its approach towards Europe, Chinese cyber actors have proven extremely adept at collecting secrets and advanced technology from both public and private sectors.¹⁴ Like Russia, China also possesses deep expertise in propaganda

and social (media) manipulation. As Chinese interests diverge from those of Europe and EU member states, there is a growing risk that it will resort to hybrid tools, including economic leverage and Information Confrontation. For now however, Beijing is heavily dependent on economic engagement with European states and is therefore much more cautious towards them than Moscow. It is anticipated that China will remain a primary European concern in terms of cyber collection and economic influence. Economic leverage will likely become a more frequently used tool for China to employ against European interests.¹⁵

The Democratic People's Republic of Korea Remains a Regional Actor with Only Limited Hybrid Capabilities to Affect Europe

Although the Democratic People's Republic of Korea holds malign intent towards the West and has the capability to inflict damage or cause disruption, it doesn't pose a major hybrid threat to Europe in the near term. It is assessed to have limited hybrid capabilities, in terms of carrying out multiple, concurrent, and sustained activities across various domains, that could disrupt European cohesion. Pyongyang's main strategic goals remain regime survival and, in conjunction with this, establishing and maintaining a credible nuclear deterrent. Besides the lingering threat of a demonstrated capability to conduct lethal chemical attacks abroad, the most credible threat that the Democratic People's Republic of Korea can employ against EU member states is from its cyber capabilities. Although much of these are employed in revenue-generating criminal activities, Pyongyang has demonstrated

14 National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace*. Washington, DC: Office of the Director of National Intelligence, 2018.

15 Van der Putten, Frans Paul, Minke Meijnders, Sico van der Meer and Tony van der Togt, eds. *Hybrid Conflict. The Roles of Russia, North Korea and China*. The Hague: Clingendael Institute, 2018, p. 28-43.

Strategic Alert

its capability to conduct destructive cyber operations against Europe.¹⁶

Outlook

Russia currently remains unrivalled in its intentions and capabilities to use hybrid tools against Europe. Moreover, Moscow likely judges that its hybrid efforts have yielded effective results. Consequently, the frequency and sophistication of these challenges is expected to increase, even when attribution is reliably pinned to Russia. Russia will continue seeking fissures within and among EU member states, and will try to exploit any opportunities to erode Euro-Atlantic cohesion. Russian hybrid efforts will likely increase in the so-called 'near abroad' and in the Western Balkans, especially in states that approach accession within Euro-Atlantic institutions, as preventing NATO and EU expansion in these regions remains a strategic goal for Moscow. These hybrid activities will increase Russia's capability to employ both direct and indirect actions, in particular its ability to more closely synchronize these activities across a greater spectrum of national institutions, while concurrently keeping these activities non-attributable, thereby complicating effective responses from European states. As the Kremlin faces increasing internal pressure, it could conduct more aggressive hybrid actions, to include cyber targeting of critical infrastructure, more provocative activity by the Intelligence and Security Services, aggressive civil society engagement aimed at exacerbating fissures and existing tensions within EU member states, and an increased penetration of media environments to advance Russian narratives. Contrary to Russia, China continues to view its international security interests from an economic angle, placing top priority on access to markets and resources and the security of economic corridors, which calls for long-term stability and a business-friendly

strategic environment. Towards Europe, China will continue to employ more subtle hybrid techniques, in particular offering states massive financial benefits and the creation or rejuvenation of infrastructure projects. However, these activities, although financially attractive to its recipients, create political leverage that support China's interests. The Democratic People's Republic of Korea will continue to pose only a limited hybrid threat against Europe.

16 Van der Putten, Frans Paul, Minke Meijnders, Sico van der Meer and Tony van der Togt, eds. *Hybrid Conflict. The Roles of Russia, North Korea and China*. The Hague: Clingendael Institute, 2018, p. 15-26.

About the Clingendael Institute

Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.

www.clingendael.org
info@clingendael.org
+31 70 324 53 84

 @clingendaelorg
 The Clingendael Institute
 The Clingendael Institute

About the author

Danny Pronk is Senior Research Fellow Strategic Foresight. His research focuses on strategic foresight and the Strategic Monitor.

Disclaimer

This report was commissioned by the Netherlands' ministries of Foreign Affairs and Defence within the PROGRESS framework agreement, lot 5, 2017. Responsibility for the contents and for the opinions expressed rests solely with the authors. Publication does not constitute an endorsement by the Netherlands' ministries of Foreign Affairs and Defence.