2022-03-21

The 5×5 -- Russia's cyber statecraft

Handler, Simon P.; Jasper, Scott

Atlantic Council

Belarus **Conflict** **Cybersecurity** **Disinformation** **Intelligence** **Internet** **Russia** **Technology & Innovation** **Ukraine**

The 5×5 | March 21, 2022

The 5×5—Russia's cyber statecraft

By **Simon Handler**

*This article is part of **The 5×5**, a monthly series by the Cyber Statecraft Initiative, in which five featured experts answer five questions on a common theme, trend, or current event in the world of cyber. Interested in the 5×5 and want to see a particular topic, event, or question covered? Contact **Simon Handler** with the Cyber Statecraft Initiative at **SHandler@atlanticcouncil.org**.*

On February 25, just a day after Russia launched a massive invasion of Ukraine, the Russia-based Conti ransomware group publicly **declared** its allegiance to the Kremlin. The cybercriminal organization said in an online post that in response to any potential attack against Russia, the group would use "all possible resources to strike back at the critical infrastructures of an enemy." Conti almost immediately revised the post to reflect a moderately softer stance, but the group had already tipped its hand to reveal what many experts have long speculated to be true—Russia-based cybercriminal organizations play an important role in the Kremlin's cyber statecraft.

To better understand what this and other recent cyber developments related to the war in Ukraine indicate about Russian cyber behavior, we brought together five experts to share their perspectives.

#1 What role do non-state actors play in Russian cyber statecraft?

Scott Jasper, *senior lecturer, Naval Postgraduate School in Monterey, California; Author of **Russian Cyber Operations: Coding the Boundaries of Conflict***:

The views presented are his and do not necessarily represent the views of the Department of Defense, the Department of the Navy or the Naval Postgraduate School.

"US Treasury Department **sanctions** on Evil Corp, a Russia-based cybercriminal organization, revealed that the group's leader, Maksim Yakubets, worked for the Russian Federal Security Service (FSB), providing further evidence the government enlists cybercriminals. US officials **feared** ransomware groups could be contracted by the Russian government to interfere with the 2020 US presidential election, especially after seeing TrickBot operators note which infected computers belonged to election officials. The concern was significant enough for US Cyber Command to temporarily take down TrickBot's command and control infrastructure."

Rafal Rohozinski, *principal, The Secdev Group*:

"Cybercriminal groups have played an important proxy role for Russia's projection of its cyber power. Apart from serving as a fertile recruitment ground for cyber talent, criminal groups are shielded from prosecution effectively granting them a license to conduct activities outside of Russia's borders. Russian business and internal politics have a rich tradition of "black propaganda" and therefore information operations including disinformation and misinformation are a powerful and present element that has been exercised many times within Russia's sphere of influence and abroad."

Gabby Roncone, *technical analyst, Cyber Espionage team, Mandiant*:

"Non-state actors continue to play pivotal roles in Russian cyber statecraft. Russia has:

1) coopted criminal groups to contribute to espionage collection, such as the criminal group Buhtrap which switched to almost exclusively cyber espionage operations after their tools were **leaked** in 2016;

2) adopted and/or modified criminal malware for use, such as the BlackEnergy malware originally developed by Cr4sh and then customized and **used** by Sandworm in the 2015 attacks on the Ukrainian power grid; and

3) sanctioned the cyber activities of Russian criminal actors against certain targets of interest to the Russian state, including groups like Conti, which we have recently learned through the Conti leaks **cooperated** with the FSB.

Russia extends a long leash to most cybercriminal actors if they refrain from targeting Russian organizations. The disruption and cost to Western organizations from these criminal operations serves Kremlin interests, even when not directed or endorsed by the state. Russian intelligence is afforded distance and plausible deniability from these cyber operations, thus using cyber criminals as proxy or mercenary actors. In addition, Russia can absorb and deploy existing cyber capabilities without expending significant additional resources to support them."

Roman Y. Sannikov, *head of cyberthreat intelligence, TRM Labs*:

"It is pretty clear that Russian intelligence agencies have used at the very least, tools developed by cybercriminals to further their political agenda. But it is much more likely that they have actually used the services of the various Russian-speaking threat actors. In some cases, the threat actors knew who they were working for and why. In other cases, it appears that they may have been unwitting accomplices."

Justin Sherman, *fellow, Cyber Statecraft Initiative*:

"Russia's cyber power is not just about the military and security services proper, though the foreign intelligence service (SVR) and military intelligence agency (GRU) have demonstrated that they have sophisticated capabilities. The Kremlin's cyber power also draws from the large, often opaque, quite complex network of proxies at its disposal, from cybercriminals to patriotic hackers to front companies. There is no single formula for understanding this entire web; for example, some cybercriminal organizations work closely with the Russian security services on a regular basis, while others are recruited by the FSB on an extremely ad hoc basis. The point is, if we are looking at the Kremlin's cyber and information operations, we cannot just focus on people in the government."

#2 How should the crossover between Russian state and cybercriminal operations influence US strategy toward Russia?

Jasper: "Headline ransomware attacks diminished after US President Joe Biden **gave** Russian President Vladimir Putin a list of off-limits critical infrastructure in Geneva in June, and the FSB even **raided** the REvil group in January 2022 at the request of US authorities. Now that severe sanctions have been levied against Russia for the invasion, there is no reason for Putin to further restrain Russian-based ransomware groups from attacking critical infrastructure in the United States. Putin may even employ them for retaliation or **revenue** generation."

Rohozinski: "Prior to the invasion of Ukraine disentangling cybercriminal operations from deliberate state backed operations was complex owing to the challenge of attribution and the likelihood that this would result in deterrence or successful prosecution. At the present time, all cyberattacks originating from the Russia Federation—whether state-backed or criminal—should be treated as a hostile act."

Roncone: "I think US Cyber Command's recent strategy of disrupting cybercriminal operations through defending forward and persistent engagement has been quite interesting and has a solid use case against Russian criminal operations that may be state sanctioned or state sponsored. This strategy seems to have played out well during the focus on disrupting ransomware operations in the lead up to the 2018 and 2020 elections. Though it is hard to tell the exact effects of these Cyber Command operations, degrading and denying these operations and making it challenging for actors to successfully operate seemed to be somewhat impactful, despite the fact that the effects did not seem to last long. From the policy side of things, in my opinion, sanctioning the criminal actors operating these cyber operations has little effect. Though it may disincentivize individual Russian criminals from malicious cyber activity, I would argue it has little to no impact on the Russian state's decision to use cybercriminal operators to further the state's interest abroad. Most Russian cyber criminals remain in Russia, which de facto negates any effect from these sanctions."

Sannikov: "For a time, US law enforcement was quite open in its collaboration with Russian law enforcement such as the FSB and MVD, as well as agencies of other post-Soviet countries. Eventually, the US agencies realized that they were helping Russian law enforcement, essentially, identify assets that could be flipped not so much to collaborate against other criminals, as is frequently done in the United States, but to go after political targets both inside and outside Russia. The **Yahoo hack** is a great example of that. While I believe that the United States will have to continue to work with Russia in some capacity in order to target criminal enterprises, right now, the effectiveness of that will largely depend on the outcome of the war in Ukraine and how that impacts Putin's regime and inner circle. I still believe that the United States could have strong partners in Russia who are ultimately interested in fighting cybercrime, but it is going to be much harder to find them under the current regime in Russia."

Sherman: "The US government must recognize that the Russian government sees the Internet in a fundamentally different way. The Kremlin also does not orient its entire doctrine and thinking around the term "cyber" as we do, and its distinctions between data (machine-readable 1s and 0s) and information (human-readable content) are not as firm as they are in the United States. US policymakers dealing with Russian state and cybercriminal operations—whether trying to help businesses defend against them, or trying to get Putin to curtail ransomware attacks launched from within Russia—must spend more time appreciating the nuances of the Russian government's view on the Internet, its complicated and deliberately overlapping use of state and proxy hackers, and its other motivations to keep cybercrime a large and economically lucrative enterprise in Russia."

#3 What role do Belarus-linked groups play in support of Russia's cyber operations?

Jasper: "Ukraine **believes** a hacking group linked with Belarusian intelligence, working with or at the behest of Russia, defaced seventy central and regional authority websites with threatening messages and installed wiper malware in government agency computers around January 14, 2022. Since the invasion, this group known as UNC1151, is believed behind a **spear-phishing** campaign targeting European countries aiding Ukrainian refugees, using compromised Ukrainian military accounts."

Rohozinski: "The term 'Russian hacker' is often thought of as referring to hackers from the Russian Federation. But in fact, it more appropriately reflects hackers who speak Russian and come from many countries and regions. In the past week, we have seen polarization within these groups between those supporting Russian actions in Ukraine, and those that are opposed. While Belarus possesses a significant technical community, including hackers, their loyalties, as of now, are unknown."

Roncone: "We currently do not know if UNC1151 cooperates with or supports Russian cyber espionage efforts. Though Belarusian targeting and collection requirements are likely very similar to those of Russia, we lack visibility into whether UNC1151 is sponsored by, working with, trained and tasked by, or acting in some way as proxy for the Russian security services. That being said, Belarusian and Russian strategic goals in the security space increasingly aligned and the two states have close security cooperation beyond the Collective Security Treaty Organization (CSTO).

There are two main factors that might influence enhanced cooperation in cyber operations between the countries: Russia's explicit support of the Lukashenka regime since the 2020 Belarusian elections and the increasing amount of loans given to Belarus by Russia over the last year. These factors likely play into why we are seeing Belarus abdicate their once close-held territorial sovereignty to host Russian troops invading Ukraine. As Lukashenka has lost legitimacy as president of Belarus and been rejected from closer ties with Europe, he is gravitating toward much closer relations with Russia. Given the current situation, I would not be surprised to discover a developed or emerging relationship between Russian and Belarusian cyber operations in the future."

Sannikov: "While Belarus has always had its share of talented cybercriminals (I am friends with a couple of them), there does not seem to be indication that they are nearly as apt to collaborate with the government either in Belarus or Russia as are Russian based cybercriminals. To date, I do not think actors based in Belarus have played a major pro-Russian or pro-Belarus role. They seem to be much more independent-minded."

Sherman: "Since Putin launched an illegal war on Ukraine, it has become clear that the Lukashenko regime in Belarus is launching cyber and information operations on behalf of the Kremlin. There are also open questions, as Gavin Wilde and I **explored**, around Russian-Belarusian entanglement in cyberspace in general, including with respect to Russian and

Belarusian internet surveillance systems and the extent to which Russian state hackers materially support or provide knowledge to Belarusian state hackers. The world must watch these kinds of Russian government cyber and information partnerships in the coming years."

More from the Cyber Statecraft Initiative:

Targeting Ukraine through Washington: Russian election interference, Ukraine, and the 2024 US election

Countering ransomware: Lessons from aircraft hijacking

Broken trust: Lessons from Sunburst

#4 Is there a particular example that typifies the "Russian" model of cyber operations?

Jasper: "The model is named information confrontation, which aims to influence the perceptions of the target audience by informational-technical and -psychological effects. A particular example is the 2017 **NotPetya**mock ransomware

upon Ukraine, attributed to a military unit in the Russian Main Intelligence Directorate. NotPetya spread through multiple propagation methods at lightning speed to damage critical infrastructure, including banks, automated teller machines and card payment systems in retailers and transport, and inflict pain upon the populace."

Rohozinski: "Russian cyber power is far more diffuse than that of the United States. The capabilities come for a wide range of actors including criminal gangs, advertising agencies, and private individuals. In the United States, the Department of Defense and Cyber Command source talent from a range of defense contractors. In Russia, this talent pool is wider and more diverse. Russian cyber operations are also typically more entrepreneurial, where groups can align their activities to what they perceive to be cues from the political leadership and, in the case of ransomware, keep the proceeds of their operations. There also seems to be competition between different intelligence and defense agencies, often going after the same target. It is also difficult, sometimes, to ascertain what the ultimate objective of a cyber operation might be, apart from having conducted it. This suggests that impressing the leadership may be more important than achieving a tangible objective."

Roncone: "In my opinion, there is no straightforward Russian model of cyber operations. I would instead delineate some of the models of cyber operations by each of the intelligence agencies sponsoring them; their varying mission mandates and cultural identities dictate these differences, though there may be overlaps in some cases. Turla, a cyber espionage group sponsored by the FSB (and my personal favorite group) looks very different than Sandworm or APT28, which are sponsored by the GRU, for example. Of course, criminal cyber operations sanctioned by or on behalf of the state look very different as well. I will say that one defining feature of Russian cyber operations is the psychological aspect to many of them—evident in many Sandworm operations in particular, such as their attacks on Georgia in October 2019, as Sandworm operations have contained a destructive element and thus are inherently meant to be seen. Even Turla, though, leaves small easter eggs for researchers during their operations, especially in their malware."

Sannikov: "I think that there has been so much collaboration on so many different levels that it is hard to find one or two typical examples. As I already mentioned, the Yahoo hack was a good example of Russian law enforcement working with cybercriminals, essentially tasking them, to hack a private company, most likely in order to target domestic opponents who used Yahoo email accounts. But frequently, the collaboration is not clearly tasked. I have spoken with Russian cybercriminals who have mentioned that, if they come across a target that they think would be of interest to Russian intelligence, for example, access to a foreign military system, they will sell or trade that to Russian intelligence for remuneration, or in exchange for "cool tools" to use for their criminal activities."

Sherman: "There are many instructive examples of Russian cyber operations, but analytically speaking, I generally do not think that we should pick one to be 'the' model case study. Even the framing of the question, concerning 'cyber' operations as opposed to 'cyber and information' operations, reflects somewhat of a Western perspective, where we make harder distinctions than Moscow between, say, hacking into a government system and spreading propaganda about that government. Of course, there is great value in studying individual Russian cyber operations for a number of reasons, including from historical, operational, and tactical perspectives. But from a strategic perspective, it is important to focus on the patterns and motivations that underpin Moscow's actions here, such as with deniability and obscurity, and to recognize that a single operation cannot be considered a blueprint for everything else or everything to come."

#5 Has the current war in Ukraine changed your perception of Russia's cyber behavior? How?

Jasper: "No, on February 15, 2022, a distributed denial of service **attack** took down websites of the Ministry of Defense, Armed Forces of Ukraine, Ukrainian Radio, and online services of state-owned Oschadbank and PrivatBank, including automated teller machines. The White House claimed **technical** evidence was linked to Russian Main Intelligence Directorate infrastructure. The assault was meant to cause alarm before the invasion, a mark of information confrontation. Low-level phishing continues in favor of kinetic assaults in a classical form of siege warfare."

Rohozinski: "What was been missing was any significant cyber component to the initial stages of the Russian invasion of Ukraine. Apart from two cases of destructive malware, the cyber 'Pearl Harbor' that everyone expected did not materialize. In part, this may have been a function of Ukraine being much better prepared in 2022 than it was in 2014. It also may signal the degree of acrimony and division within the Russian cyber community, between those supporting Putin's objectives, and those opposed. It may also speak to the way the Russia's military establishment views the utility of cyber operations. For the most part, cyber operations are the domain of intelligence. Cyber was certainly not

synchronized with the movement of almost 200,000 Russian troops into Ukraine. Heavy metal, rather than bits and bytes, seem to be in the forefront of Russian general planning and leading the campaign. This may change in the days ahead. But for now, cyber is a whimper and not a bang."

Roncone: "It has. The most impactful cyber operations we have seen from Russia so far have been mainly disruptive or destructive attacks. They seem to be using older, more primitive tactics, techniques, and procedures to achieve this (such as DDoS, defacements, basic wipers), and these attacks appear to have had somewhat limited effects. I think a lot of people, including myself, expected to see more novel techniques leveraged during this time to include a more coordinated strategy aligned with ongoing military and kinetic operations. It is interesting to see the contrast between the new Sandworm tool released by the UK National Cyber Security Centre, **Cyclops Blink**, which is supposedly Sandworm's new version of VPNFilter, and the relatively rudimentary wiper operations conducted in this conflict so far. We have to keep in mind, though, that this war is in its early stages and thus perhaps we can guess these cyber operations may be in their early stages as well."

Sannikov: "While I am a bit surprised at how little damage has been done by Russia's offensive cyber-operations, overall, I'm not too surprised. While "Russian hackers" are quite good. As we have seen, they are by no means infallible. Russian intelligence is dangerous because it is persistent and malicious. As we've seen in numerous examples, like some of the deadly poisonings in the UK, they are by no means superspies. In many ways, more Austin Powers villains than John LaCarre villains."

Sherman: "I think it is too early to answer that question. For a multitude of reasons, I am very hesitant—and believe that we should all be very hesitant—to draw sweeping conclusions about "the role of cyber in conflict," about "Russia's cyber strategy," and other related issues right now. We are only a few weeks into what is unfortunately poised to be a very long conflict; we are analyzing information in the public source, doing so amid the fog of war, and in a war with tons of disinformation and propaganda circulating. It is easy to jump to conclusions, but it is important to recognize what we do and do not know at this time (for the latter, that is a lot). I also think that we should recognize the biases that can come with studying a particular field: when you study cyber capabilities all day, it is easy to want to imagine that cyber is the most important thing in warfare and entirely ignore, for example, the continually important role of kinetic military capabilities that directly and immediately kill people. And from a preparedness and risk assessment standpoint, we must recognize that Moscow is not taking anything off the table, and just because it has not launched the massive, destructive cyberattacks some imagined would happen yet does not mean it will not engage in more aggressive or damaging cyber behavior in the coming weeks or months."

Simon Handler is a fellow at the Atlantic Council's Cyber Statecraft Initiative within the Scowcroft Center for Strategy and Security. He is also the editor-in-chief of The 5×5, a series on trends and themes in cyber policy. Follow him on Twitter ***@SimonPHandler****.*

The Atlantic Council's **Cyber Statecraft Initiative**, within the Scowcroft Center for Strategy and Security, works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology.

LEARN MORE

Related Experts: **Justin Sherman**

Image: Flag of Russia on a computer binary codes falling from the top and fading away. Credit: iStock/Gwengoat