Russian Federation

August 2017

Chief of State:	President Vladimir Vladimirovich Putin
Government:	Semi-Presidential Federation
Capital:	Moscow
National Holiday:	12th June[1]
GDP by sector:	Agriculture (4.7%), Industry (33.1%), Services (62.2%)
Export Partners:	Netherlands 11.9%, China 8.3%, Germany 7.4%, Italy 6.5%, Turkey 5.6%, Belarus 4.4%, Japan 4.2%
Import Partners:	China 19.2%, Germany 11.2%, US 6.4%, Belarus 4.8%, Italy 4.6%[2]
Top Exports:	Mineral fuel including oil (47.2%); Iron & Steel (4.9%); Gems & precious metals (3.1%); Machinery including computers (2.4%); Fertilizers (2.3%); Wood (2.3%); Aluminum (2.1%); Cereals (2%)[3]
Conflict areas:	Syria, Ukraine, NATO and Allies, Chechnya, Georgia
Major Religions:	Christianity, Islam

Current Landscape

International Relations

The Russian Federation has conducted itself in a far more assertive manner than has previously been observed post the fall of the Soviet Union. In 2008, Russia engaged in open warfare with Georgia. In 2014, Russia seized and annexed Crimea, followed by overall intervention in Ukraine[4]. In 2015, Russia deployed forces to Syria to aid the regime of Bashar al-Assad. This was the first "out-of-area" military operation since independence [5]. There has also been bold retaliation towards uncooperative states, most recently involving the expulsion of 755 US diplomats from their diplomatic posts in response to a US sanctions bill [6]. Russia has repeatedly tested defences by sending aircraft into European airspace, and most recently staged a Naval celebration day that included Chinese warships as part of the demonstration. Russia desires to be seen as an alternative to the NATO-led West for other nations. Russia has used both economic and military power to exert pressure. Russian state-owned gas giant Gazprom has wielded influence over the politics and economics of many European countries[7].

Internal security posture

Putin's leadership as President has seen marked efforts to increase internal surveillance and controls. This has taken the form of new legislation to "weaken independent civic actors… with selective prosecutions aimed at intimidating society", "discrediting foreign-

[1] The 12TH of June is when Russia celebrates the establishment of Russia as an independent country after the collapse of the Soviet Union in 1991

[2] https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html

[3] http://www.worldstopexports.com/russias-top-10-exports/

[4] https://www.csis.org/programs/russia-and-eurasia-program/russian-foreign-policy

[5] https://www.foi.se%2Freport-search%2Fpdf%3FfileName%3DD%253A%255CReportSearch%255CFiles%255C5fa9f89b-8136-4b15-9aaf-1d227aee90a0.pdf&usg=AFQjCNFwq_p2BnEcUB9sc4GXApGRoQ_54Q

[6] http://www.independent.co.uk/news/world/americas/us-politics/vladimir-putin-donald-trump-sanctions-russia-usa-crimea-diplomats-expelled-moscow-a7868096.html

[7] https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

funded groups" and efforts to "fund and promote apolitical and pro-government organisations" [8]. Freedom House has given the country an aggregate "freedom score" of 22 out of 100 [9]. Unpunished violence against journalists has contributed to violations against media freedom. The "Yarovaya Law" has included new powers that provide the state authorities with the ability to repress religious groups for the purpose of fighting extremism [10]. Legal repercussions for expressing opinions online have also increased. As an example, in 2016 Alexsei Kungurov was sentenced to two years in a penal colony for criticizing Russia's actions in Syria[11].

Economy

Despite a weak external environment, the Russian economy was predicted to grow at a rate of 1.3% in 2017[12]. During 2016, low oil prices and sanctions over Ukraine negatively impacted the Russian economy before finally taking a turn towards recovery at the end of the year. Russia is one of the world's leading energy exporters, making the fall in commodity price and high inflation particularly tough on ordinary households[13]. The Financial Times reported that Russia's climb out of recession has brought the forecast for gross domestic product growth up to 1.5%. Putin has outlined an interest in building a "digital economy" in areas such as "big data, artificial intelligence and virtual reality."[14] A recent visit from the German Chancellor Angela Merkel to Russia highlighted the importance of cooperation between the two countries in economic terms. Germany features as a major import and export partner for Russia. Despite the topic of sanctions not being brought up, Russia is currently having to contend with threats from the US around fresh sanctions. Although recovering, new sanctions could further thwart the only recently recovering Russian economy.

National Cyber-Strategy

According to the Centre for naval Analysis (CNA), Russian military theorists use the term "informatsionnaya voyna," or information warfare, over the popular use of "cyber" or "cyberwarfare". The national doctrine uses a broader understanding of information warfare, which sits along other more traditional weapons such as "disinformation operations, PsyOps, electronic warfare and political subversion"[15]. The Swedish Defence Agency reported in 2010 that "several organisations are responsible for handling information warfare capabilities" whilst the FSB and the GRU are most likely to be operating Russian offensive and defensive capabilities[16]. The FSB is believed to maintain and operate SORM, the states internal cyber surveillance system[17].

GRU

FSB

SVR

Russia's most recent "National Security Strategy" does not use the term "cyber" at all. Instead, it uses phrases such as "information sphere," "Information security" and "information infrastructure". There are a number of entries pertaining to the recognition of information and communication technologies as a source of national security risk, as well as inferences as to the strengthening of controls. The 2015 "Military Doctrine of the Russian Federation" highlighted the need "to enhance capacity and means of information warfare" and recognised that there are "subversive information activities against the population, especially young citizens of the State, aimed at undermining historical, spiritual and patriotic traditions related to the defense of the Motherland"[18].

[8] http://carnegieendowment.org/2017/05/18/delegitimization-and-division-in-russia-pub-69958
[9] https://freedomhouse.org/report/freedom-world/2017/russia
[10] https://freedomhouse.org/report/freedom-world/2017/russia
[11] https://pen.org/press-release/russian-blogger-sentenced-to-two-years-in-prison/
[12] http://www.worldbank.org/en/country/russia/overview#3
[13] https://www.weforum.org/agenda/2016/12/things-to-know-about-russia-s-economy/
[14] https://www.ft.com/content/206d3a7a-47b0-11e7-8519-9f94ee97d996
[15] www.dtic.mil/get-tr-doc/pdf?AD=AD1019062
[16] http://www.highseclabs.com/data/foir2970.pdf
[17] www.dtic.mil/get-tr-doc/pdf?AD=AD1019062
[18] https://rusemb.org.uk/press/2029

The Main Intelligence Directorate (GRU)

Head:	Korobov Igor Valentinovich
Minister Responsible:	Sergey Shoygu, Defense Minister
Parent Agency:	Ministry of Defence
Headquarters:	119160, Moscow (Ministry of Defence), Khodynka Airfield (GRU) “Aquarium”
Type of Service:	Central intelligence agency of the Armed Forces
Areas of Concern:	Military; Military-political; Military-technical; Military-economic and Environmental spheres.[19]
APT Groups:	APT28, also known as “Sofacy”, “STRONTIUM”, “Pawn Storm”, “Tsar Team” and “Fancy Bear”. (Although attribution for APT28 has been disputed between GRU and FSB, APT28 has largely been reported as originating from Russia’s military intelligence unit — GRU)[20].
Other Groups:	Yemen Cyber Army, Cyber Berkut, Cyber Caliphate (Groups that have been purported to be a front for the Russian GRU)[21,22].

The Federal Security Service (FSB)

Director:	Alexander Vasilievich Bortnikov
Headquarters:	Lubyanka Square, Moscow, Russia
Type of Service:	Russian internal security and counterintelligence service
Areas of Concern:	Counterterrorism; Border Security; Maritime Security, Economic and Resource Security; Information Security
Subdivisions:	PR; Department of material and Technical Support; Military Counterintelligence; Medical Directorate; Antiterrorist Center; Investigations; Centre for Specialist Techniques; International Cooperation; Radio Intelligence; Operational and Technical Measures; FSB Security; Open information Department; Academy.[23]
APT Groups:	APT29, also known as “Cozy Bear” has been previously attributed to the federal security services (FSB)[24,25].

The Service of Foreign Intelligence (SVR)

Director:	Naryshkin Sergey Evgenievich
Headquarters:	Yasenevo, Moscow, Russia
Type of Service:	The Foreign Intelligence Service of the Russian Federation
Units:	Operational; Analytical and Functional
Subdivisions:	Director’s Staff; Department of protocol; Academy; PR and Media; Operational; Office of Analysis and Information; External Counterintelligence; Informatics; Scientific and Technological revolution, Management of Operators, Economic Intelligence, Support services.[26]

[19] http://structure.mil.ru/structure/ministry_of_defence/details.htm?id=9711@egOrganization

[20] https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

[21] https://www.intelligence.senate.gov/sites/default/files/documents/os-trid-033017.pdf

[22] http://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand/

[23] www.fsb.ru/

[24] http://www.ecfr.eu/page/-/ECFR208_-_CRIMINTERM_-_HOW_RUSSIAN_ORGANISED_CRIME_OPERATES_IN_EUROPE02.pdf

[25] https://cyberx-labs.com/en/blog/dhsfbi-report-says-russian-cyber-units-attacked-critical-infrastructure-blackenergy/

[26] http://svr.gov.ru/index.htm

Russian-Based Organised Crime

Organised crime thrives in the right ecosystem. There is a growing body of evidence that Russian-based organised crime (RBOC) has links to the SVR, GRU and FSB. In the past, crime groups have been used as tools of the state to conduct intelligence activity[27]. Today, RBOC accounts for approximately a third of heroin in Europe, a large amount of human trafficking and illegal weapons imports. Political and business affiliations, used to facilitate the efficacy of organised crime, have likely helped RBOC to grow. Belarus (for example), a key Russian export/import partner, has a large spread of Russian community and business connections in local politics[28]. The same approach has been seen between cyber-criminals and the state security services. Talent in the right skillsets has been notoriously difficult to acquire globally, but not when there is already a culture for collaboration internally between underground actors and the state[29]. This approach enables Russia to conduct operations with plausible deniability. It is also worth noting that Russian criminals have the benefit of both virtual and physical safe-havens. Eastern European countries and Russia do not have extradition treaties with the West, and as long as the criminals do not attack Russian infrastructure they have largely been protected[30].

Interpol defines cybercrime into two different areas:

- Advanced cybercrime (or high-tech crime)
- Cyber-enabled crime

Technology and the dark web have been widely adopted by criminals to conduct activities. This is evidenced by the large number of online markets selling access to drugs, weapons and other illegal products and services. Russian carding sites follow this trend, providing access to sensitive financial information as well as sharing tools and tricks to help advance other would-be criminals repertoire of abilities. This type of activity would be categorised as cyber-enabled crime. On the other hand, sophisticated attacks, such as those linked to Carbanak Gang and the FIN campaigns, fall under the category of "advanced cybercrime". It is not difficult to draw linkages between traditional organised crime (their advancement in methodologies) and current trends in cybercrime. It is therefore not surprising that such a potent region for organised crime also has a hefty reputation for conducting cybercrime.

The US "most wanted" list contains a number of individuals believed to be located in Russia or Ukraine[31]:

Name	Crime	Last seen/ Potential residence
Ivan Viktorvich Klepikov	Zeus Malware	Russia, Ukraine
Alexey Dmitrievich Bron	Zeus Malware	Russia, Ukraine
Vyacheslav Igorevich Penchukov	Zeus Malware	Russia, Ukraine
Evgeniy Mikhailovich Bogachev	Zeus Malware	Russia
Igor Anatolyevich Sushchin (FSB Officer)	Large scale intrusion	Moscow, Russia
Dmitry Aleksandrovich Dokuchaev (FSB Officer)	Large scale intrusion	Moscow, Russia
Alexsey Belan	Large scale intrusion	Krasnodar, Russia

[27] https://www.theregister.co.uk/2017/06/06/russia_cyber_militia_analysis/

[28] http://www.ecfr.eu/page/-/ECFR208_-_CRIMINTERM_-_HOW_RUSSIAN_ORGANISED_CRIME_OPERATES_IN_EUROPE02.pdf

[29] https://bpr.berkeley.edu/2017/04/07/cybercrime-the-spark-which-started-russias-cyber-crusade/

[30] https://www.thecipherbrief.com/article/tech/crimicon-valley-russias-cybercrime-underground-1092

[31] https://www.fbi.gov/wanted/cyber

Civil society and its discontents

Just as RBOC can be used to "outsource" the mission objectives of the state, so too can hacktivism be weaponised for motives that benefit the government. Russia is not alone in this thought process; protest groups and activism have been carefully interfered with in the past by many states. The activity allows them to enhance an agenda or justify further actions. In the "information sphere" this has taken the guise of groups such as the "CyberCaliphate," which hacked into TV5 Monde in France[32], and "Tsar Team" (previously linked to apt28) leaking information about athletes' medical histories. The Ukrainian based "Cyber Berkut" has been a feature of attacks against pro-European institutions and national infrastructure during the conflict. The "Yemen Cyber Army" (YCA) has also been accused of having been created by the same organisation behind APT28 (FSB)[33]. Information taken from the Saudi Ministry of Foreign Affairs (after being hacked by the YCA) was then published on WikiLeaks.

Psychological operations (PsyOps) and social media have also played a role in influencing the "perceptions, attitudes and behaviours of target populations". This can be done by spreading rumours, usually by exploiting already embedded dislikes and prejudices, fear and exploiting hopeful wishes for possible outcomes[34]. Russia has been accused of using this tactic via social media to influence the outcomes of the US elections. The activity forms a basis for why sceptics are unsure as to why the Kremlin would have wanted Donald Trump in the White House[35]. Disinformation forms a part of this process and groups such as Cyber-Berkut have been using strategically placed "leaks" to further pro-Russian rhetoric[36, 37]. They have also leaked information that discredits Hillary Clinton in the past, outlining her relationship with Ukrainian billionaire Victor Pinchuk[38]. The FSB 16TH Center and 18th Center were found to be behind an internet propaganda effort directed at Ukraine; Ukrainian news sites were controlled by Russia and anti-Ukrainian activists[39].

One way to generate mass amounts of disinformation is the use of bots, which can be used to swamp social media. For example, activists in Turkey and Syria were subject to "bot spamming campaigns" in an attempt to drown out oppositional influence[40]. Bot spamming was allegedly used during the first US presidential debate, when 37.7% of pro-Trump tweets (22.3% pro-Clinton tweets) were suggested to have been from bots.[41]

نحن قادمون
#OpSaudi
We Don't Forget
We Don't Forgive
"Operation Hussein Badreddin al-Houthi"
MOFA.GOV.SA Hacked By YEMEN Cyber Army

[32] https://securelist.com/files/2016/10/Bartholomew-GuerreroSaade-VB2016.pdf
[33] https://securelist.com/files/2016/10/Bartholomew-GuerreroSaade-VB2016.pdf
[34] https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Lange_Svetoka_12.pdf
[35] http://time.com/4783932/inside-russia-social-media-war-america/
[36] https://www.wired.com/2017/05/russian-hackers-using-tainted-leaks-sow-disinformation/
[37] https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/
[38] https://www.cyberscoop.com/cyberberkut-returns-hillary-clinton/
[39] https://autoblog.postblue.info/autoblogs/lamaredugoffrblog_6aa4265372739b936776738439d4ddb430f5fa2e/media/e69ef19e.FSB-IO-UKRAINE.pdf
[40] http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/02/Comprop-Working-Paper-Hwang-and-Rosen.pdf
[41] http://comprop.oii.ox.ac.uk/

Future Concerns

In light of Russia's assertive foreign policy and willingness to conduct information warfare, there are some predictive areas which may see either direct attacks or more subtle influence:

European elections

There are a number of European elections in 2017. If it is the case that European democratic uncertainty or the right government can help Russia achieve its strategic goals, the likeliness of interference in the campaigns up to and during the elections should be considered likely. Because certain economies are more important to Russia, it is more likely that these are the ones Moscow will be observing carefully and attempting to manipulate. The following elections are set to take place:

- Norwegian parliamentary election, 11 September 2017
- German federal election, 24 September 2017
- Catalan independence referendum, 1 October 2017
- Portuguese local election, 1 October 2017
- Austrian legislative election, 15 October 2017
- Czech legislative election, 20-21 October 2017
- Danish local elections, 21 November 2017
- Slovenian presidential election, November 2017
- Georgian local elections, 2017
- Estonian municipal elections, 2017

The outcome of Germany's election will be important as they are a substantial export and import partner. Russia was reported to have hacked into the German parliamentary systems in 2015[42] and Germany's pro-immigrant stance was also undermined by fabricated stories of rape published in Russian media[43]. It would be prudent to observe if any candidates stand out as being more sympathetic to Moscow, or as being outliers capable of undermining confidence and observing potential PsyOps.

Balkans

Russia has stepped up its hybrid warfare tactics in the Balkans. This was seen in Montenegro previous to its recent successful application to NATO when in 2016 the country was victim to an orchestrated coup[44]. Montenegro sought support from Britain as it faced cyber-attacks on the day the coup was supposed to take place, and then again in February this year[45]. Russian media outlets targeted Montenegro citizens with campaigns several weeks before the Parliamentary elections in October 2016, depicting the country's leadership as "corrupted, bribed and a pawn of the US and NATO"[46]. An uptick in Russian cyber activity is increasingly likely as NATO deployments expand in surrounding areas, and Russian military presence increases respectively. The Balkans sits precariously between these rival regions of influence. Due to the encroaching influence of NATO in the region, and Russia's failed attempt at dissuading Montenegro from joining the NATO alliance, retribution in the form of continued interference is a strong possibility. NATO was undermined by lack of coherent support when Crimea was annexed. Russia will attempt to posture and send a strong signal to the Balkan region. Kosovo falls within this vulnerable group as it has sought NATO membership as well.

Central Europe and the Baltic states

Estonia and Latvia are recognised as being particularly vulnerable to any attempt at a Russian fuelled Hybrid-war or even conventional war. They are already NATO members, but there are concerns that Russia will seek to use Russian minorities to gain influence[47]. This is likely to take the same Modus Operandi as other previously articulated attempts to interfere; PsyOps, electronic attacks aimed at spreading disinformation and discrediting or undermining current leadership. The form of interference might be ambiguous, which serves to thwart a confident stance from NATO and the EU. This would further undermine the credibility of the US.

[42] http://www.bbc.co.uk/news/technology-36284447

[43] https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf

[44] https://csis-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/ts170713_Samp_testimony.pdf?yGQ2Mn4EWBPNYQLN3A367gqqqoXpojVf

[45] https://cyber-peace.org/wp-content/uploads/2017/03/Montenegro-asks-for-British-help-after-cyber-attacks-in-wake-of-Russian-backed-coup-plot.pdf

[46] https://www.ft.com/content/cab4c2de-72a1-11e7-93ff-99f383b09ff9?mhq5j=e1

[47] https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf

The four “Visegrad” countries (Poland, Hungary, Czech Republic and Slovakia) are a group of Central European nations that have a shared history, including a communist past and Soviet occupation. Russia exerts broad internal influence in these countries through its regional energy policy, diplomatic activity and information warfare. A study on the vulnerability to subversive influence places Hungary as the most vulnerable to “hostile foreign influence”[48]. In Hungary, it appears that the ruling party “Fidesz” has positioned itself as openly pro-Russian since 2010[49, 50]. It is Russia’s role in the energy sectors of these countries that helps further their influence[51]. Poland is the least susceptible to this type of influence from Russia.

The Unites States and the Kremlin

The foreign relations between the US and Russia have turned rapidly frosty. During the first week of August President Donald Trump signed a bill into law that levies new sanctions on Russia. Trump has largely been seen as a President that does not seek to label Russia as an “enemy”[52]. This law however, prevents President Trump from lifting the sanctions or returning two US-based Russian diplomatic compounds. Russia retaliated against the sanctions by announcing 755 American diplomatic staff are to be expelled, and two US diplomatic properties seized[53, 54]. Although supported by US congress, the decision to impose sanctions has not been met with the same confidence in Europe. Germany and Austria detailed concerns in a joint press release. This is likely to be because of anxieties over the planned “Nord Stream 2 gas pipeline”[55].

The economic future of Russia, which has been markedly affected by previous sanctions, affects other European countries too. This conflict of interests will likely continue as the impact of the sanctions is felt moving forward. Because Russia seems to have felt there was a possibility of the sanctions being lifted, the new bill may be seen as a betrayal. As a result, it is unlikely that Russia will cease seeking to undermine US economic interests in Europe and abroad. This activity will likely take a number of forms to continue Russia’s strategic plans:

- Proxy cyber wars fought between the two regions are a possibility in areas of strategic significance;
- Economic espionage to hinder or steal an advantage from competing companies affected by the sanctions;
- Direct retaliation in order to exert influence over the US and its decisions.

All possibilities are converged due to the consequences of the sanctions in Europe. Meaning that European countries will also have to make decisions as to their own position, and subsequent accepted risk of retaliation from Russia. The real impact of this issue remains to be seen.

About the Author

Sara Moore (smoore@anomali.com) is a Cyber Threat Intelligence Analyst at Anomali.

[48] http://www.cepolicy.org/publications/vulnerability-index-subversive-russian-influence-central-europe-0
[49] http://www.riskandforecast.com/post/in-depth-analysis/russia-s-far-right-friends_349.html
[50] http://foreignpolicy.com/2017/03/30/the-real-russian-threat-to-central-eastern-europe-2/
[51] https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf
[52] http://russiancouncil.ru/en/news/riac-urban-breakfast-is-there-a-future-for-russia-us-relations-/
[53] http://www.aljazeera.com/news/2017/07/russia-expels-755-diplomats-response-sanctions-170730201720880.html
[54] https://www.nytimes.com/2017/07/30/world/europe/russia-sanctions-us-diplomats-expelled.html
[55] https://www.ft.com/content/cab4c2de-72a1-11e7-93ff-99f383b09ff9?mhq5j=e1