An Oxford Analytica Briefing Book

The Rīga Conference 2020

Online, November 12 – 13, 2020

Oxford Analytica

THE RĪGA CONFERENCE 2020

CONTENTS

Contact us: T +44 1865 261600 (North America 1 800 965 7666) or oxan.to/contact

Rīga Conference delegates:

In a world of growing complexity and change, with threats and opportunities multiplying, objective analysis of geopolitics, macroeconomics, technology, public policy and society is indispensable for decision-makers worldwide.

It is our pleasure to provide you with this Briefing Book in support of the Riga Conference 2020. These selected articles, drawn from the Oxford Analytica Daily Brief, provide analyses on the key topics addressed in the meeting agenda.

Founded in 1975, Oxford Analytica is an independent geopolitical analysis and advisory firm. Our mission is to help our clients navigate complex markets where understanding the intersection of politics and economics, business and society is critical to success. We combine our global network of 1500 experts with high-calibre in-house analysts who deploy robust methodologies and build collaborative relationships to deliver trusted, impartial, actionable insights. Today, we work with many of the world's most influential businesses, governments and international organisations.

If you have any questions arising from any of the articles included here, or would like to know more about our services at Oxford Analytica, please contact us.

Your sincerely,

Francois Deschamps,
Senior Vice President
Oxford Analytica

François Deschamps
Senior Vice-President
fdeschamps@oxford-analytica.com

Russia reviews Karabakh priorities to remain relevant

Tuesday, October 27, 2020

Smoke rises over Stepanakert, Karabakh, after Azerbaijani artillery shelling (AP/Shutterstock)

A fast-developing conflict is forcing the Kremlin to look at how to restore stability and retain regional dominance

Moscow will try to limit the damage to its interests and prestige as renewed fighting around Nagorno-Karabakh forces it to adapt to shifts in the regional balance of power, frozen since a 1994 ceasefire. Russia previously focused on maintaining the status quo in the Armenian-Azerbaijani stand-off for want of better options, but changes in military control on the ground and Turkey's new assertiveness may force a change of attitude.

What next

Russia will seek to contain Azerbaijan's military successes, minimise Turkey's role in military operations and in conflict resolution and keep an increasingly disgruntled Armenia on side. One practical way of achieving all this would be to deploy peacekeepers under an international mandate, an idea now being discussed seriously.

Subsidiary Impacts

◦ While diplomacy continues, territorial advances and evidence of atrocities will make it difficult to ensure truces are adhered to.

◦ Iran will offer to help mediate but will avoid further involvement if possible; no outcomes other than stability are good for it.

◦ Relations between Armenia and Israel will suffer because of the latter's arms deliveries to Azerbaijan.

Analysis

Baku's military successes present a major challenge to the multifaced approach Russia has taken until now. This has involved:

- retaining Russia's position as security guarantor for Armenia but maintaining good relations with Azerbaijan;
- maintaining the status quo in place since 1994, where Armenian forces control Nagorno-Karabakh and seven adjoining districts, rather than permitting changes through military action; and
- pursuing negotiations through a multilateral rather than unilateral format: the US-Russian-French-led Minsk Group of the Organisation for Security and Cooperation in Europe.

President Vladimir Putin's remarks at the annual Valdai Club meeting on October 22 illustrate the dilemma of how to remain even-handed without undermining Russia's historical patronage of Armenia. Without naming perpetrators, Putin recalled "the enormous tragedy of the Armenian people during the First Word War" and the "brutal crimes" committed against Armenians in Sumgait in 1988 and later in Karabakh.

At the same time, he said, "a situation where Azerbaijan has lost a significant part of its territory cannot continue forever" (see RUSSIA/CAUCASUS: Putin hones Karabakh diplomacy - October 23, 2020).

Calibrated support for Armenia

Armenia is formally bound to Russia in the Collective Security Treaty Organisation (CSTO) and Eurasian Economic Union (EEU). Russia argues that it is not obliged to defend Armenia under the

The downing of a combat plane inside Armenian airspace on September 29, Baku's admission that it destroyed missile launchers in Armenia on October 11 and any future incidents must raise questions about this policy; the CSTO charter views an attack on one member state as an attack on all, requiring action (see RUSSIA/CAUCASUS: Moscow pushed towards firmer stance - September 30, 2020).

Many in Yerevan believe Russia should have offered Armenia more support, given the long-standing bonds between them. Some suspect this reticence stems from antipathy towards reformist Prime Minister Nikol Pashinyan, who came to power in 2018 on the back of mass protests and prosecuted former officials close to Moscow.

Ultimately, Russia will not want to weaken its political, economic and security ties with Armenia. Nor does Yerevan have other realistic options, however it views Russia's approach to the conflict. Both Putin and Pashinyan stress that they are in frequent contact.

Managing Azerbaijani expectations

Azerbaijan has refrained from joining the CSTO and EEU and has built oil and gas ties with Europe through Turkish pipelines bypassing Russia. Nevertheless, both states proclaim their exemplary relations, and Moscow has been happy to sell Baku weapons as well as arming Yerevan.

Maintaining the post-1994 balance, including by means of arms sales to both states, was already looking less sustainable as Azerbaijan used its oil wealth to source high-tech weaponry from Turkey and Israel.

> Moscow must decide whether to acknowledge changes in military control

The changing geopolitical calculus may force Moscow to review its stance and accommodate itself to Azerbaijan's unfolding military advances. This may involve acknowledging Azerbaijan's capture of some Armenian-held districts outside Karabakh itself, perhaps in the Fizuli-Hadrut-Jebrail strip along the Iranian border where fighting has been particularly fierce.

Curbing Turkish ambitions

Turkey's growing assertiveness -- openly encouraging Azerbaijan to capture Karabakh by military means -- and its desire for a presence at the negotiating table create new challenges for Moscow (see CAUCASUS: Allegiances collide in Karabakh conflict - October 22, 2020 and see AZERBAIJAN/ARMENIA: External moves key to conflict - October 2, 2020).

At the Valdai meeting, Putin acknowledged fundamental differences with Turkey on Karabakh, but framed them in the broader context of a "reliable partnership" and asserted that he could work through difficult issues with Turkish President Recep Tayyip Erdogan.

Russia has stated clearly that the Minsk Group format must remain the sole format for conflict resolution, with no role for Turkey (see RUSSIA/TURKEY: Moscow shuts Ankara out of Karabakh - October 13, 2020). Despite multiple disagreements with Washington in other spheres, Putin says he believes "100%" that Russia's US and French partners are committed to the same peaceful outcome (see US/CAUCASUS: Joint diplomacy pushes for Karabakh truce - October 21, 2020).

If Russia can engage Baku more and correspondingly weaken Turkish influence, it may be in a position to draw Azerbaijan into considering greater EEU and CSTO involvement, while seeking to curtail Turkish military assistance for the Azerbaijani military.

In such a scenario, Azerbaijani President Ilham Aliyev might be less insistent on including Turkey in the It is by no means certain that such a rebalancing effort would be effective. If Aliyev suspects that

Russian recognition of territorial gains is designed to 're-freeze' a modified 1994 status quo, prevent further Azerbaijani advances and avoid more Armenian territorial losses, he could grow resentful and move closer to Ankara, risking more direct (but probably still covert) Turkish military involvement.

Peacekeeping proposal

One possible route to enhancing direct Russian influence could be a peacekeeping deployment. This idea has been floated periodically over the years, but has been voiced as a realistic prospect in the current conflict. From Moscow's perspective, it would have the immediate advantage of marginalising Turkey from the conflict.

A peacekeeping mission might be Russia's least bad option

Kremlin spokesman Dmitry Peskov has said peacekeepers are an option if the warring parties agree to this.

Yerevan and Baku resisted the idea prior to the current conflict. However, Pashinyan said on October 22 that a peacekeeping deployment would be "acceptable and Foreign Minister Zohrab Mnatsakanyan has said the idea is under discussion.

Aliyev said in an October 22 interview that "we don't reject it in principle" although there were many questions to be resolved including timing and mandate. He carefully used the broader formulation "observers or peacekeeping forces".

Outlook

A peacekeeping deployment could entrap Russia more in the intractable Karabakh dispute, with an intervention it has avoided over many years despite its willingness to engage militarily in Ukraine, Georgia and Syria. Now it may offer the best solution in the circumstances by:

- freezing open warfare and prevented escalation into direct war between the Armenian state and Azerbaijan;
- de facto granting Azerbaijan control of some extra territory;
- shutting out Turkey; and
- for the first time, securing an international mandate for a foreign deployment (from the Minsk Group).

If successful, a deployment could allow the dispute to lapse into more years of torpor with neither side making the concessions needed to move towards a resolution of Karabakh's final status: independence, restoration to Azerbaijan or something else.

Russia and China lead on offensive cyber skills

Thursday, July 23, 2020

Western governments have attributed several cyberattacks to government-linked actors in Russia and China

A man typing on his computer in Warsaw (Reuters/Kacper Pempel)

Over the past week, Western governments have attributed several offensive cyber campaigns to Russian and Chinese state-linked actors. Although public 'naming and shaming' has become a common practice since the 2017 WannaCry malware attack, damaging cyber campaigns show no signs of decreasing.

What next

Russian and Chinese offensive cyber operations will become more sophisticated as the two sides develop their capabilities. The reluctance of Western countries to follow up on attribution statements with proportionate penalties risks adversaries perceiving them as soft targets.

Subsidiary Impacts

- Cyber actors will use 'false flag' operations, using tools linked to different units to confuse their targets and delay their responses.
- China is showing a willingness to subcontract cyber campaigns to criminal proxies.
- COVID-19 research will be the prime focus of cyberespionage until a vaccine comes on the market.

Analysis

The United Kingdom on July 16 attributed breaches of Oxford-based COVID-19 vaccine research facilities to APT-29, a hacking group linked to Russia's Foreign Intelligence Service, the SVR (see INTERNATIONAL: COVID-19 alters focus of cyberespionage - June 11, 2020). The UK statement was backed up by Canada and the United States, which are also part of the Five Eyes intelligence sharing alliance together with Australia and New Zealand.

Oxford researchers supported the attribution when they revealed the same day that they had noticed their Russian counterparts were taking a similar approach to vaccine development.

Also on July 16, the UK foreign secretary revealed that Russia had tried to interfere with the 2019 general election by stealing and leaking documents on UK-US trade discussions online.

On July 21, a UK Intelligence and Security Committee report called Russia an "urgent" national security threat due to its willingness to deploy its sophisticated cyber capabilities "in a malicious capacity" (see INT: UK report on Russian meddling has broad impact - July 21, 2020).

These public attributions have drawn attention to Russian offensive capabilities.

Russian capabilities

According to the UK National Cyber Security Centre (NCSC), APT-29 enters digital networks by using publicly available 'exploits' to scan them; the purpose of this is to obtain authentication credentials that can give hackers deeper access into the networks.

It uses a broad targeting method, meaning it likely maintains a store of credentials, which may not be relevant presently but could be useful in the future. In the case of COVID-19 vaccine research facilities, APT-29 ran a basic vulnerability scan against the IP addresses owned by the facility, after which it deployed public exploits against the vulnerable services that it had identified.

This malware was previously not known in the public domain and had not previously been used by Russian state-actors. This underlines the sophistication of the new tools Russia is developing and deploying against the high-stakes target.

APT-29 receives little publicity compared with other Russian threat actors because it focuses on covert intelligence collection. In contrast, APT-28, which is reportedly linked to Russia's GRU military intelligence agency, has conducted much bolder and more destructive campaigns.

APT-28's operations indicate that it employs skilled developers and frequently uses 'zero days' -- vulnerabilities that are unknown and for which patches do not exist.

APT-28 and APT-29 are believed to be two of the most capable cyber actors in the world. They were also linked to the breaches of the US Democratic National Committee (DNC) in 2016. APT-28 has been linked to the hack of French TV station TV5 Monde in 2015.

China's skills

The US government on July 21 indicted two Chinese hackers, who worked with the Ministry of State Security (MoSS), for conducting a decade-long operation against companies engaged in high-tech manufacturing, pharmaceuticals and gaming software development.

The indicted persons are said to have also targeted dissidents, clergy and human rights activists in the United States, China and Hong Kong. Their latest mission was to probe vulnerabilities in the networks of companies working on COVID-19 vaccines, treatments and testing technology.

The indictment is significant in that it describes the hackers as working partly for personal financial gain and partly as state proxies.

From the information provided in the indictment, their methods do not seem especially sophisticated: to gain access to the target networks, the hackers exploited known vulnerabilities in popular web server software. They were effective because the vulnerabilities had only recently been publicly revealed, and many companies and users would not yet have had a chance to install new patches.

'Cloud Hopper'

Chinese cyber theft of Western intellectual property is a longstanding concern. The most notorious cyberattacks include the 2015 hack of the US Office of Personnel Management and the 'Cloud Hopper Operation' discovered in 2018. The latter involved several Chinese operatives including a highly skilled MoSS unit known as APT-10.

> China's Ministry of State Security is a highly capable offensive cyber actor

These groups conducted a multi-year operation in the systems of the world's leading cloud service providers, including Ericsson, Hewlett Packard, IBM and Fujitsu, for gathering economic intelligence and intellectual property. However, the capabilities of the units involved varied considerably, with some seemingly stealing files at random.

The 'Five Eyes' group of intelligence-sharing governments attributed the operation to China in December 2018. Many details of the breach have been withheld at the request of the corporate victims, who fear reputational damage and loss of client confidence. This reluctance hinders attempts to deter the adversary and stop future attacks.

China is leveraging this reluctance as it builds its cyber capabilities; currently it lags Western skills in many areas, including innovation capabilities, cyber military strength and the coherence of the national cyberspace strategy.

President Xi Jinping wants China to become a 'cyber superpower'. Beijing has also created the Strategic Support Force under the People's Liberation Army (PLA). The unit is still being developed but could eventually prove to be one of the PLA's most valuable capabilities.

Western strategy

Western states boast highly sophisticated cyber capabilities, as shown by the Stuxnet operation, believed to have been launched jointly by the United States and Israel. In 2018, Washington adopted a new strategy which allows US Cyber Command to conduct persistent operations to challenge adversarial activities, including by reaching into the networks of hostile countries.

UK agencies have also conducted offensive cyber operations against Islamic State actors.

However, Western state-linked actors face transparency and accountability pressures from which their Russian and Chinese counterparts are free. Western actors also lack the same incentives to steal intellectual property.

Consequently, Western governments have focused on attribution since 2017, with limited impact (see PROSPECTS H2 2020: Cybersecurity - June 4, 2020).

The Russian ambassador to London rejected the most recent UK allegation about Russian hacking, even though the NCSC said it was 95% certain in its attribution of the Oxford hack. With this kind of certainty, cyberattacks are no longer plausibly deniable.

> Attribution appears to have little deterrence value

Attribution without proportionate retribution -- most of the penalties for cyberattacks have been economic and diplomatic sanctions with limited consequences -- risk portraying Western countries as soft targets that lack resolve.

Outlook

This means that offensive Russian and Chinese cyber campaigns will continue increasing as these states' capabilities develop. Russia's operations indicate that its units are more skilled at sabotage; operations often have political goals. China's focus remains on intellectual property theft and espionage for economic gain, although Russia's APT-29 is also skilled at the latter.

Russian cybercrime treaty proposal favours autocracies

Thursday, August 27, 2020

Russia is canvassing members of the UN General Assembly to support its draft of a new cybercrime treaty

Protest against tightening state control over internet in Moscow, Russia March 10, 2019 (Reuters/Shamil Zhumatov)

A UN intergovernmental group of experts is scheduled to submit its recommendations on a new Russian-proposed cybercrime convention to the UN General Assembly meeting next month. The move is part of a wider struggle among member states over the control of the internet and norms of responsible state behaviour in the cyber domain.

What next

There is no guarantee that the UN will approve the Russian cybercrime treaty. Yet deliberations over it will demonstrate that Western democracies and autocracies such as Russia and China are becoming more rather than less divided on whether the internet should be open and free or tightly state-controlled. Internet controls serve a dual function: they suppress domestic opposition and consolidate the fundamental asymmetries in the cyber domain that make open digital spaces more vulnerable than closed ones to foreign cyberattacks.

Subsidiary Impacts

- Russian will obstruct progress on any international cyber norms that advance the interests of Western democracies.
- The issue of cyber-specific rules on territorial sovereignty will become more contentious as attacks against private entities rise.
- States are increasing their reliance on proxies for cyberoperations to have a measure of public deniability.

Analysis

The UN Convention on Cooperation in Combating Cybercrime (A/C.3/72/12) proposed by Russia in October 2017 aims to counter "the use of information and communications technologies for criminal purposes".

The proposal was approved by the 193-member UN General Assembly in a 79-60 vote in December 2019 amid strong protests from European states, the United States and prominent human rights organisations.

The UN also approved the establishment of an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate such a treaty.

This committee has been tasked with deliberating on the outlines and modalities of the proposal in August and to submit recommendations to the 75th UN General Assembly, which opens in September.

Budapest Convention

Russia has framed its proposal as an alternative to the 2001 Budapest Convention, also known as the Convention on Cybercrime.

The Budapest Convention regulates and fosters international cooperation on cybercrime by harmonising national laws and improving investigative techniques. Specifically, it provides:

- common definitions and criminal prohibitions;
- unified procedures and rules to ensure evidence preservation; and

- mutual legal assistance to facilitate cooperation among signatories on cybercrime investigations.

The convention was drafted by the Council of Europe with the active participation of several observer states including the United States. It has been ratified by 65 states, including some non-European states such as Australia, the Dominican Republic, Japan, Mauritius, Panama and the United States. Notably, Russia and China have not signed it.

Closed internet

US and European officials and human rights groups have warned that the Russian proposal seeks to establish a UN treaty that would permit governments to block websites hosting material that may be critical of them and to use technologies to monitor dissidents and activists (see RUSSIA: Domestic cybercrime a growing concern - August 11, 2020).

> The critics see Russia advancing its strategic goals under the guise of leading international reform

Since the range of activities that can be covered under the "use of information and communications technologies for criminal purposes" is vague and broad, there is concern that such a treaty would be used to criminalise ordinary -- or political but non-criminal -- online behaviour in contravention of international human rights protections.

Indeed, criminalising ordinary activities of individuals and organisations through the misuse of cybercrime laws, especially against dissidents, is becoming common, according to the UN Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association.

Weakening wider norms-setting bodies

The Russian proposal is being seen by Western governments as yet another attempt by the Kremlin to obstruct progress on wider norms in cyberspace.

GGE

At present, a UN Group of Governmental Experts (GGE) is deliberating on norms for responsible state behaviour in cyberspace in the context of international security. The UN GGE consists of 25 member states and has established six working groups since 2004.

The GGE can be credited with two achievements: outlining the global agenda and introducing the principle that international law applies to cyberspace.

The non-binding 2013 and 2015 UN GGE reports determined that existing international law, in particular the UN Charter, applies to cyberspace. Consequently, it is fairly well accepted that any cyberoperation which results in an equivalent effect as traditional kinetic use of force -- prohibited under Article 2(4) of the UN Charter -- would be legally considered a wrongful use of force by a state actor.

Secondly, the International Law Commission's Articles on State Responsibility, in principle, hold a state responsible for a cybercampaign if that campaign constitutes a wrongful act and if it can be attributed to a specific state.

To date only a few states have clarified how these Articles specifically apply to state-linked cyberoperations. These include the United Kingdom, Australia, France and the Netherlands.

Many states, notably the United States, have adopted a strategic ambiguity or a 'wait and see' approach, refraining from taking a position so as not to limit their range of available operations.

OEWG

Seeing this initiative as favouring Western interests, Russia pushed for the establishment of a second UN-mandated working group in 2018. Called the Open-Ended Working Group (OEWG), it comprises all interested UN member states and is also open to participation from the private sector and international organisations.

The OEWG has undercut the effectiveness of the GGE by setting up a parallel process, complicated the structure of multilateral discussions on cyber norms and made consensus harder to achieve.

Territorial sovereignty

The lack of progress on building international consensus on norms has led to academic initiatives, notably the Tallinn Manual, on how existing frameworks of international law apply to the cyber domain.

Due to the rise in cyberattacks against individuals, private companies and government installations, a key strand of the debate is the link between state-linked cyber campaigns and territorial sovereignty.

The principle of non-intervention in international law applies to prohibit operations that involve coercive behaviour by one state that deprives the target state of its free will in relation to its exercise of sovereign functions.

This principle has, for example, been discussed regarding recent cases of electoral interference, although Russian activities in the 2016 US elections have not been classed as a breach of US territorial sovereignty by officials in Washington.

The issue has become especially salient following the rise in state-linked cybercampaigns against COVID-19-related research by university laboratories and private pharmaceutical firms (see INTERNATIONAL: COVID-19 alters focus of cyberespionage - June 11, 2020).

> Proxies complicate attribution of cyberattacks to state actors

Some states such as France and the Netherlands argue that cyberattacks against private and government entities should been viewed as breaching state sovereignty, as the targets are located within the affected state.

The criteria for the threshold beyond which an operation in cyberspace may violate another state's territorial sovereignty divides opinion, partly because espionage is not illegal under international law. Moreover, because international laws apply to states, they do not prohibit cyber operations by private actors and proxies that are not directly attributable to a state.

Outlook

For the time being, no consensus seems forthcoming. The continued lack of cyber-specific rules on territorial sovereignty works to the advantage of autocratic states such as Russia (and China) as it frees their hand to advance their foreign agenda via offensive cyber tools (see INT: Russia and China lead on offensive cyber skills - July 23, 2020) while limiting their own exposure by tightly controlling the domestic digital space.

Election interference can undermine democracies

Friday, January 17, 2020

With the US presidential elections this year, attention on the security of electoral systems is growing

Former Special Counsel Robert Mueller testifies before the House Intelligence Committee on his report on Russian interference in the 2016 presidential election, July 24, 2019 (Reuters/Chip Somodevilla)

The United States is one of many countries due to hold elections this year, amid concern over foreign interference. Although interference by domestic or foreign actors through social media has attracted most attention, hacking is a broader phenomenon that can take place at the technical level (voting machines, counting mechanisms), the infrastructure level (electoral rolls, election officials) and the social level (news organisations, political parties). Attacks are more commonplace at the infrastructure level than the technical one.

What next

The most likely electoral interference operations are disinformation campaigns -- these are hardest to defend against, and the results of the disruption most unpredictable. While governments and major social media platforms (such as Twitter and Facebook) are making efforts to stop such practices, it is likely that in some jurisdictions at least, attacks will succeed in undermining the concept of an election.

Subsidiary Impacts

- Beyond external actors, domestic political actors will also engage in disinformation as electoral strategies.
- Voters may be put off voting or question the outcome of the vote.
- Societal rifts are likely to widen due to lack of shared ground truth.

Analysis

'Election hacking' is a widely used term, covering everything from attacks on voting machinery or infrastructure, to interventions that affect the social systems underpinning the vote. Attacks can come from a variety of actors, including foreign governments and domestic opposition, as well as hacktivist organisations such as Anonymous or terrorist groups.

Hacking undermines the legitimacy of elections, weakening democracies, which are based on trust between the population and the government, and the reliability of the official vote tally.

Election hacking operations may change the political debates, influence votes through misinformation campaigns and alter the concept of reality among the electorate, but even more directly, may cause votes to be miscounted, inauthentic votes to be added, or take advantage of voting patterns to shift the outcome of the vote.

There are three primary areas where attacks can occur:

Technical level

Targets at this level include voting machines and online voting systems, software and hardware manufacturers, and election management systems.

Three of the most important templates for electronic voting come from the United States, Australia and Estonia (see INTERNATIONAL: Hacking fears to slow e-voting adoption - December 22, 2016).

United States: electronic voting machines

Transparency is generally good practice in cyber security, allowing outsiders to check that software and systems have been designed and implemented correctly. For electoral systems in particular, without independent testing of the security of voting systems it cannot be known how secure they are and what vulnerabilities they have. However, due to national security concerns, voting systems are often shielded from public inspection.

US electronic voting infrastructure is deeply insecure

In the United States, as a result, voting machines are deeply insecure (see UNITED STATES: Poll meddling defences may be too late - October 18, 2019). Information security researchers have found that:

- manufacturers of voting machines in 2018 instructed election officials to use and recycle weak passwords;
- machines in Wisconsin and Kentucky ran insecure data transfer protocols as of 2018;
- machines supposedly isolated from networks ('air gapped') in Wisconsin, Michigan and Florida have actually been connected to the internet; and
- local election authorities had poor information security practices.

Australia: mathematically verified electronic voting (vVote)

The Australian state of Victoria conducted the first fully "end-to-end verified" electronic voting in 2014. Contrary to the proprietary systems used in the United States, the Victoria system was published in peer-reviewed academic journals and is freely available for scrutiny.

Interestingly, a fundamental part of the "verifiability" was a final step in the voting process, where the voter could cause the machine to decrypt their vote, so the voter could check that the machine registered it correctly. Victoria officials felt this might undermine voter confidence in the process and decided not to advertise this step, which undermined the security of the system -- if there was a mistake or a hack, it would not be detected.

The result of that electronic vote was considered credible although vVote was only available at a subset of polling places and was optional. Only about 1,200 electronic votes were actually cast. Subsequent use of the system in Western Australia in 2017 exposed verifiability issues and vVote was not used in the 2019 federal election.

Estonia: online voting (i-voting)

Estonia has been using a version of i-voting since 2005 and, while it is imperfect, it is widely seen as the best current system for online voting: the code has been submitted to open review and adversarial testing. An independent review of operational cyber security found the system to be generally robust but security relied on a high degree of trust and communication between the people running the system. Estonia's particular circumstances may make it difficult for other countries to emulate its example (see ESTONIA: E-governance model may be unique - October 25, 2016).

Infrastructure level

Attacks at the infrastructure level (electoral commissions, electoral registers, state and local officials) are more common than attacks on technical systems. Cyber security firm FireEye has seen breaches to collect intelligence, co-opt, display false information on public-facing systems, and as part of an influence campaign. The UK National Cyber Security Centre highlights the threat of voting infrastructure becoming unavailable at key moments (such as the voter registration deadline or election day).

This has potentially happened in the United Kingdom, in the lead-up to the 2016 Brexit referendum -- the voter registration website went offline due an alleged denial of service attack. This type of attack could affect the outcome of a close vote. For example, if young people are the most likely to register to vote at the last minute, then taking the registration website offline near the registration deadline might cause a shift in the demographics of the electorate and therefore restrict votes for those parties popular with the young.

During the Ukrainian elections in March 2019, election staff experienced attacks on election servers and personal computers, and were sent fraudulent emails attempting to get victims to reveal personal information and credentials (phished). Hackers bought their personal details on the dark web. Kenya's 2017 presidential election was re-run due to a number of anomalies in the vote, including a claim that a key election management system was compromised.

Societal level

Attacks on the societal level (eg, news organisations, political parties, social media, donor groups) are difficult to attribute, increasingly common, and insidious (see INTERNATIONAL: Disinformation operations will multiply - November 20, 2019). Societal-level attacks might be designed to influence directly the outcome of an election, but can also be an attempt to create general instability, or to undermine democracy itself.

Disinformation campaigns effectively 'gaslight' a whole nation

Tools for this include disinformation, harassment, and distraction: effectively psychological manipulation ('gaslighting') on a national scale. This may make the electorate doubt their news sources or undermine the shared concept of reality, or, more simply, make people become disengaged from the process and reduce voter turnout.

Echo chambers on social media can be used as a tool to spread and distort messages in unexpected ways. Bots and troll armies can be used to amplify or drown messages on social media and give a false impression of grassroots support.

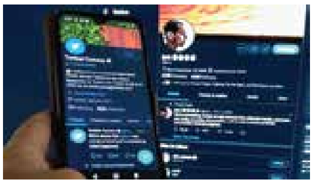
Attacks at this level include stealing information or emails and releasing them into the public domain, such as the hack of the Democratic National Committee in 2016 and email leaks from French President Emmanuel Macron's 2017 election campaign; the UK NCSC is currently investigating whether a 2019 leak of US-UK trade negotiation documents was an operation by Russia.

Simply making up information can also be equally effective as exfiltrating it for some of these groups (see INTERNATIONAL: Disinformation operations will multiply - November 20, 2019).

State disinformation operations will multiply

Wednesday, November 20, 2019

A few states lead foreign and domestic disinformation campaigns, notably Russia and China, but others are following suit



Feeds from Twitter's communications departments and its CEO Jack Dorsey, August (Reuters/Jim Bourg)

The breadth and depth of global influence operations have expanded hugely in recent years. There are now more states using information operations to further their policy goals, while the established players are deploying their toolsets against ever more targets.

What next

More countries will conduct information and influence operations on social media as the barriers to entry become lower. Much of this will involve black-market or third-party service providers, which will impede attribution and may lead to false accusations against states where the companies are located. Russia and China, the largest players, will expand the scope of their operations and focus on platforms, countries, and languages where the moderation policies and platform policing are less well developed.

Subsidiary Impacts

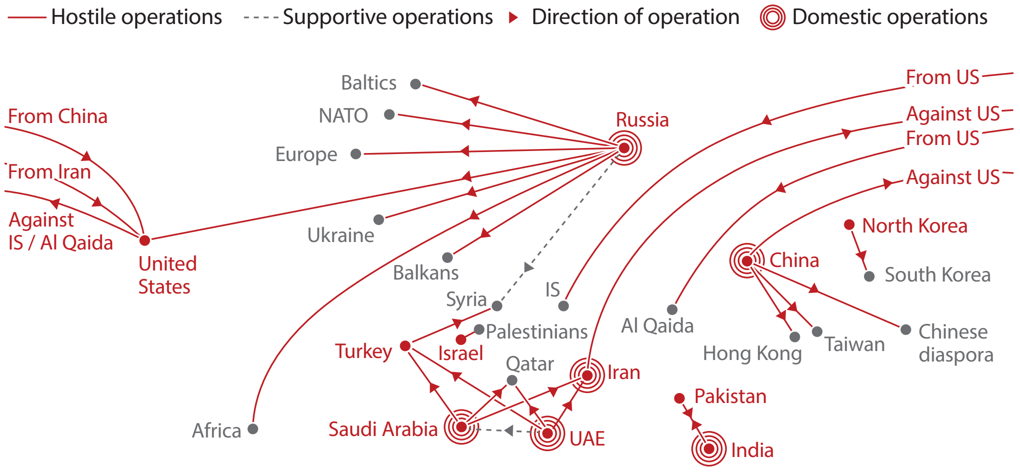
- Politicians will increasingly label legitimate criticism as foreign interference.
- The success of Russia's actions in the 2016 US election and lack of coherent response have emboldened other states to replicate its tactics.
- In the future, information operations may be met with a stiffer response to prevent this perception of weakness.
- During conflicts, information operations will become a key aspect, with all sides trying to control the narrative on social media.

Analysis

Organised social media manipulation campaigns took place in 70 countries in 2019 -- an increase of over 30% from 2018 and more than twice that seen in 2017, according to the Oxford Internet Institute (see INT: Governments step up social media capabilities - October 22, 2019).

The two largest social media platforms, Facebook and Twitter, have publicly attributed information operations to seven countries: China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela. On top of this, there is evidence that North Korea, Israel, Turkey, Brazil, Sri Lanka and the United States practise information operations.

Major state-sponsored disinformation operations (as of 2019)



Graphic: Oxford Analytica

Russia

Evidence suggests that Russia has been manipulating its domestic information environment since 2009, targeting Russian audiences on social media. The St Petersburg-based Internet Research Agency (IRA) is the most active organisation, infamously targeting the 2016 US election; however, the military intelligence agency (GRU), is also increasingly active.

Domestic operations

Information operations primarily focus on domestic audiences. Analysis of IRA content in Russian compared with English shows that Russian language accounts are more specialised in their messaging, pushing messaging that echoes state policy and seeks to build cohesion.

Conversely, messages targeted abroad push both sides of opposing narratives seeking to drive polarisation. Narratives are broad and deliberately confused and contradictory, aiming to cloud the information space and obscure the truth. Often local embassies have been involved in spreading disinformation online through official Twitter accounts.

Targeting the United States

The best-known information operation on social media is that of the IRA targeting the 2016 US election. Social media messages sought to divide users on topics of race, police brutality, political candidates and other social issues. Fake accounts targeted both sides and sought to polarise debate. Research suggests that these attempts were successful. This messaging did not stop with the 2016 election but continues and will likely target the 2020 US election (see UNITED STATES: Poll meddling defences may be too late - October 18, 2019).

Targeting Europe and NATO

Russian social media campaigns against Europe have been similar to those targeting the United States; the aim is to sow and exacerbate division. There is evidence they targeted the 2017 French presidential elections and the 2016 Brexit campaign (see EU/RUSSIA: Moscow aims to widen divisions - May 2, 2019).

Activity has also concentrated on undermining support in Western Europe for NATO deployments to the Baltic States and Poland, as well to destabilise Turkey's political and security cooperation with both Europe and NATO.

Moscow aims to engage with Russian-speakers in its 'near abroad'

Within the Russian 'near abroad' (Estonia, Latvia, Lithuania, Moldova, Belarus), and increasingly the Balkans, narratives for the titular populations focus on inefficiency, corruption and the ineffectiveness of NATO, whereas for native Russian-speakers they criticised host governments and the West for failing to protect their interests.

Targeting Ukraine

Ukraine has been the testing ground for Russian information operations since the annexation of Crimea in 2014. The tactics developed there have subsequently been deployed elsewhere. Automated and semi-automated troll accounts and fabricated news websites have pushed narratives portraying the crisis in Ukraine as having been instigated by the Ukrainian government, and accused Ukrainian policy of being fascist or supportive of neo-Nazi ideas.

As recently as July 2019, Facebook removed nine IRA pages with a total of 30,000 followers that targeted Ukraine with pro-Kremlin messaging and divisive content. They focused on religious conflict, pro-Kremlin narratives surrounding the Second World War and the 2014 Ukrainian revolution.

Targeting Syria

Russia has also been conducting information operations in Syria in support of the Assad regime and against its opponents. This has included attacking NGOs such as the White Helmets and spreading conspiracy theories.

Targeting Africa

The Stanford Internet Observatory in October showed that Russia is increasingly targeting African countries (especially Libya, the Central African Republic, the Democratic Republic of the Congo, Madagascar, Mozambique and Sudan), looking to shape the continent's politics and to increase Russia's economic opportunities as a response to Western sanctions.

China

After Russia, China is the second-largest actor in information operations. It is widening both the breadth of targets and the scope of tactics used, although at times the narratives can be somewhat simplistic, primarily portraying a utopian and saccharine view of China.

Targeting domestic audiences

As in Russia, most activity has targeted domestic audiences to quell opposition and promote pro-government content.

Beijing hires locals en masse to post online pro-China content

Beijing's approach however differs from Moscow's: research suggests that as many as 2 million Chinese may be hired to post pro-government messages on social media, flooding message boards and dominating the conversation, rather than engaging in meaningful debate to change users' opinion. As evidence of scale, in mid-October, pro-Chinese accounts posted 16,000 messages in 12 hours against the NBA's Houston Rockets general manager, who had voiced support for protests in Hong Kong -- with evidence suggesting these were real people behind the keyboard, not bots.

Targeting Taiwan

Recently, Beijing has started pivoting towards targets outside mainland China (see CHINA: Disinformation activities may spread abroad - November 19, 2019).

The first of these has been Taiwan, where the policy goal is to bring Taiwan closer to mainland China. This campaign has included promoting pro-Chinese candidates in the 2018 Taiwanese local elections with inauthentic social media campaigns.

Targeting Hong Kong

In response to pro-democracy demonstrations in Hong Kong during 2019, Beijing conducted an extensive online campaign to portray protesters in a negative light; ranging from allegations of association with Islamic State (IS) to portraying individual protesters as cockroaches. Much of the activity has been conducted on Facebook and Twitter, which are blocked in mainland China. This activity therefore appears intended for a wider global audience in order to sway perceptions of the protesters overseas.

Estimates suggest that hundreds of thousands of social media accounts may be involved. Many of these accounts were purchased on the black market from commercial operators and before being re-purposed they were previously pushing business-related spam content.

Targeting the United States

There are suggestions that China has targeted the United States for disinformation. Following Trump's announcements of trade war hostilities, advertisements run by Chinese state-funded news outlets began to target US users: pushing Chinese ideas regarding the trade war and tariffs, and claiming that the tariffs are hurting the United States more than China.

In September 2018, the US administration put out a statement claiming that China was interfering in the 2018 US mid-term elections; however, this activity was shown to be paid advertising in Chinese-owned newspapers rather than covert social media activities.

Targeting the Chinese diaspora

Chinese individuals living overseas have been a major target of information operations. There is a broad campaign to promote the Communist Party's general view of China and the world, and to prevent Chinese businessmen from defecting to the United States.

> Beijing targets both Han nationals abroad and ethnic minorities

Ethnic minorities are also targeted: Beijing uses WeChat to contact and monitor Uighurs living in Europe as part of an effort to collect intelligence and shape the behaviour of Uighurs globally.

Iran

Iranian operations are designed to push issues and narratives in line with Iranian foreign policy. Much of the uncovered content has promoted themes hostile to Saudi Arabia and Israel, and favourable to the Palestinians, as well as support for alternative US policies which are favourable to Iran. The conflict in Syria, and Saudi Arabia's war in Yemen, have also been focal points.

Targeting domestic audiences

The vast majority of Iran-linked pages target Iran itself rather than overseas targets. Pro-regime narratives cover the Israel-Palestine conflict and proxy conflicts with Saudi Arabia. Content also criticises the People's Mujahedin of Iran (MEK), a political opposition group.

Targeting the United States

Iran has also targeted US politics. Its campaigns have promoted anti-Republican, pro-Democrat and pro-liberal content, as Trump's election resulted in the cancellation of the 2015 nuclear deal and new sanctions on Iran (see IRAN: Oil blockages risk military escalation - October 28, 2019).

Iran does not seem to create as much original content as either Russia or China, and instead relies on recycling or promoting genuine content that matches its policy goals, including from left-leaning activist groups, fringe media and conspiracy websites.

Other foreign targets

Beyond Iran's primary foreign targets (Saudi Arabia, Israel and the United States), content is also promoted in a broad range of languages and across a wide span of regions. Languages include Arabic, Hindi, English, Indonesian, French, Farsi, Hebrew and Spanish. More recent Iranian operations had a particular focus on Indonesia, India, Nigeria and Egypt.

Pakistan

The primary focus of Pakistani information operations is India.

Up until April 2019 the Pakistan Army ran a network of Facebook and Instagram pages which sought to inflame tensions with India, push Pakistan's claim over Kashmir and boost support for Pakistan abroad. The pages derided India and used actual events as trigger points for this criticism.

> India and Pakistan primarily aim disinformation operations at each other

India

Indian social media operations are primarily focused towards a domestic audience.

Domestic targets

Most posts are about local news and politics, including upcoming elections. Automated social media accounts have been particularly active around election periods.

Targeting Pakistan

There is limited evidence of information operations originating from within India that target Pakistan in response to operations directed at them, but attribution is unclear.

United Arab Emirates (UAE)

The UAE is active in targeting Qatar, Iran and Turkey whilst posting messages of support for Saudi Arabia. Many of the campaigns pursue these goals in an interconnected way without a clear distinction between campaigns.

Saudi Arabia

A number of Saudi-run social media operations linked to the state-run media aim to imitate independent news organisations to target domestic audiences and amplify narratives beneficial to the Saudi government.

Targeting Turkey, Qatar, Iran

Foreign campaigns from Saudi Arabia have attempted to undermine Turkish President Recep Tayyip Erdogan for his stance on Israel and the conflict in Syria, and to attack the ruling family of Qatar. Anti-Iran narratives have also been pushed to Arabic-speaking audiences (see GULF STATES: Offensive cyber tools have regional focus - April 30, 2019).

Saudi Arabia targets specific critics in disinformation campaigns

Campaign against critics

Riyadh also engages in a combination of social media accounts, fake websites and malware distribution services which have targeted individuals critical of Saudi Arabia regardless of their host nation.

Venezuela

Since 2010, Caracas has been running a substantial information operation to shape political debate in the country. This has involved automated social media accounts that promote supporters of President Nicolas Maduro and pro-government narratives.

Increasingly, Venezuela is also borrowing tactics from Russia and using actual events as hooks with which to spread particular messages or to highlight pro-government achievements.

Overseas targets

There is evidence of a slight shift towards foreign policy-focused information operations. These include support for Cuba and the Bolivarian Alliance of the Americas (ALBA), and against the US Free Trade Agreement of the Americas (FTAA). Pro-Maduro social media accounts have also been found to be active within Chilean protest conversations, but whether this is linked to a state-run operation is unclear.

North Korea

The Korea Institute of Liberal Democracy, a Seoul-based think tank, estimates that North Korea has approximately 7,000 personnel employed to manipulate online opinion through websites, blog posts, video content, and online commentary. This effort appears mainly targeted towards South Korea with the intention to promote North Korean ideology and military capability.

Within North Korea, domestic internet access is rare, and the majority of citizens cannot access social media. Much social media output is therefore targeted towards the international community, aiming to improve North Korea's image on the global stage. This is often focused around large geopolitical events such as the 2019 meeting between Trump and President Kim Jong-Un.

Israel

Israel was one of the first adopters of the use of information operations on social media, but they have mainly focused on supporting military operations, primarily in Palestinian territories. During the 2012 Operation 'Pillar of Defence' the Israel Defence Forces (IDF) published real-time updates on social media with the aim of garnering international support.

Overseas

In August, a smartphone application 'Act.IL' was launched in Israel. It amplifies communications from both the Israeli Defence Forces (IDF) and Israeli Ministry of Foreign Affairs. It also promotes civil society groups that are supportive of Israel among the Jewish diaspora living abroad.

Israeli firms offer disinformation campaigns for a fee to other states

Private sector

Israel has a growing private sector that engages in information operations for commercial clients. In May 2019 Facebook removed 265 Facebook and Instagram accounts originating from Israel which focused on manipulation of the information environment in Nigeria, Senegal, Togo, Angola, Niger, Tunisia, Latin America and Southeast Asia.

United States

The United States has been involved in conducting information operations for a number of years. All of the publicly released material is in support of military operations. In 2003 Operation Iraqi Freedom successfully used mass media to shape public opinion surrounding the military campaign in both the United States and Iraq. More recently, information operations have targeted Al Qaida in Afghanistan and IS in both Iraq and Syria.

It is unclear if the United States is involved in wider disinformation operations. It is possible that it does not engage in them, or is adept at hiding its tracks. The latter could involve agreements with US-based social media not to disclose operations even if identified.

Other states

Many other states are starting to use information operations on social media to further their international goals. This includes Turkey in support of itsoffensive in north-eastern Syria and Brazil on domestic economic and political events, as well as Sri Lanka and Egypt (see BRAZIL: Government through social media raises risks - May 17, 2019).

The proliferation of information operations across the globe means that more countries than ever are looking to manipulate the social media environment for geopolitical gain or to further their foreign policy interests (see INT: Online disinformation campaigns will proliferate - April 11, 2019).

Western pushback against China will increase

Monday, October 12, 2020

China's relations with the West are the worst they have been in decades

The aircraft carrier USS Ronald Reagan heads for the South China Sea (US Navy/ZUMA Wire/Shutterstock)

US President Donald Trump used his speech at the UN General Assembly last month to attack China over COVID-19. Senior US officials see Communist-led China as the foremost threat to the United States. The Trump administration's campaign against it spans the spectrum of government actions: criticism; tariffs; sanctions; regulatory crackdowns; military intimidation; support for Taiwan; and restrictions on imports, exports, investment and visas.

What next

The hardening of US policy to China predates Trump and is likely to continue, regardless of who wins the November presidential election. A similar dynamic is apparent in other Western states, portending greater confrontation and rivalry. China will find more receptive partners in developing states in Latin America and Africa, although these cannot fully substitute for the United States and Europe in light of China's economic and political interests.

Subsidiary Impacts

- Beijing will have little success in driving a wedge between Washington and its major Western allies.
- The West is unlikely to produce a convincing alternative to the Belt and Road Initiative (BRI).
- Negative public views of China incentivise China-bashing by politicians, which in turn feeds negative public opinion in a downward spiral.
- Beijing will persist in its efforts to encourage a more positive view of China among Western publics.

Analysis

The Party sees the West, and Washington in particular, as its most serious external threat.

On the individual level, Chinese attitudes to the West are ambivalent. Admiration for Western popular and traditional culture coexist with resentment over colonial aggression, hegemony and perceived racism. Many Chinese covet Western (especially US) citizenship, aspire to emigrate, or to send their children to the West to study and eventually settle.

> Seemingly pro-Western sentiments do not preclude anti-Western nationalism

Ideological conflict

The Party rejects liberal democratic ideas as 'Western', considers them an ideological threat and works hard to counter their spread within China.

The West, meanwhile, cannot coexist comfortably with the Party, whose political monopoly affronts a deeply rooted Western belief that multi-party representative democracy with universal suffrage is the only legitimate form of government. Western governments restrain missionary impulses for pragmatic reasons, but are never likely to accept or treat the Party as an equal.

China is on the defensive in the ideological contest. Liberal democracy has appeal within China; China's political system has negligible appeal in the West. The West aspires to change the Party; the Party aspires merely to preserve itself.

China would undoubtedly like to see Western systems fail in order to reduce the appeal of liberal democracy within China. However, its influence operations have not so far attempted to undermine democracy, merely to neutralise criticism of the Party and promote China's interests.

China enjoys an asymmetric advantage in that Western societies are permeable to Chinese state media and personnel, whereas Western media and personnel are heavily restricted in China.

United States

China views US economic and military power as its benchmark for success. It aspires at least to equal it. China is the only country that can plausibly aspire to this, but still falls significantly short by most measures.

China's emergence as a leading international player in a handful of high-technology sectors (notably telecoms, online services, spaceflight and artificial intelligence) has raised alarm in Washington. Decades of heavy Chinese investment in other high-tech sectors, such as autos, passenger aircraft, medical technology and pharmaceuticals have failed to produce global brands (see CHINA: Domestic firms will gain ground in world market - October 22, 2018). Despite China's high R&D spending, its capacity for basic research is weak.

China's military cyber and space capabilities are relatively advanced, but its conventional capabilities lag significantly behind those of the United States. Its forces have no experience of modern warfare and very limited capability to operate long distances from China. Beijing has no allies besides Pyongyang and only one overseas base (Djibouti, since 2017).

China feels directly and imminently threatened by the US military. US forces fought China in the 1950-53 Korean War, killing hundreds of thousands of Chinese soldiers. In the 1950s, US nuclear power deterred Communist forces from 'finishing' the Chinese Civil War by seizing Taiwan. In the 1960s, the CIA trained and funded guerrilla insurgents in Tibet. Many Chinese believe that the US bombing of the Chinese embassy in Belgrade in 1999 was not accidental.

Washington is a treaty ally of two countries with which China has active territorial disputes (Japan and the Philippines) and an increasingly important security partner of two others (India and Vietnam). The largest overseas deployment of US troops anywhere in the world is in Okinawa, a few hundred kilometres from China. US aircraft carriers frequently enter China's near seas and US surveillance missions approach China's coasts. US arms sales and threats of intervention are, in Beijing's view, the reason Taiwan can resist pressure to 'unify' with China.

In the economic realm, Beijing does not view its subsidies, 'forced' technology transfer and cyberespionage as unfair, since it holds Western imperialism and hegemony responsible for China's relative poverty and weakness. Rules that Washington considers a 'level playing field' China views as reinforcing advantages the West already enjoys on account of being richer and more technologically advanced.

In the ideological realm, Washington welcomes and celebrates Chinese dissidents and promotes political liberalisation in China. The Party views this as aggressive and aimed at embarrassing and destabilising China.

The Communist Party considers Washington an existential threat, whereas Washington views China merely as the principal threat to US dominance -- though some officials present this as equalling an existential threat.

This is new.

In the post-Cold War era, Washington saw China as a rising power that could be socialised into prevailing Western norms through greater integration into the global economy and international institutions. It believed that China would become more liberal and that prosperity would eventually lead to democracy.

This paradigm had bipartisan support, though there were some partisan differences: in the 1990s, Democrats were more critical of China on human rights grounds, whereas Republicans prioritised preserving business ties.

The US business community no longer functions as a de facto lobby for China in Washington and Republicans have become more critical of Beijing.

The Trump administration has effectively ended decades of US ambivalence during which China's economic and military power grew without a concerted US effort to undermine them.

Polls show that negative views of China prevail and are rising steadily within both parties.

International competition

Beijing views the United States as a hegemon in long-term decline, and Donald Trump's presidency as the latest stage in this.

Trump's foreign policy has benefitted Beijing indirectly by weakening US international leadership. Washington has withdrawn from the Trans-Pacific Partnership, Paris climate change agreement and World Health Organisation. Trump has raised doubts about Washington's commitment to its allies and initiated disputes with them over trade and cost-sharing. His administration's failure to control COVID-19 improves China's image by comparison.

However, Beijing has done little pro-actively to assume international leadership, nor achieved substantial gains from Trump questioning US alliances. Australia, Japan and the United Kingdom have followed Washington's lead in banning Huawei from their 5G networks. Canada abandoned negotiations with China on a free trade agreement in 2017 when Washington insisted it would be incompatible with membership of the Five Eyes intelligence alliance. Relations between Ottawa and Beijing worsened in December 2018 over Canada's detention of Huawei's chief financial officer. Vietnam and India continue to seek and obtain closer defence cooperation with Washington in response to Chinese threats.

However, China is undercutting US influence in developing regions through its economic policies.

Developing countries in Latin America, Africa and South-east Asia have young populations eager for affordable Chinese consumer goods, particularly technology. Parts of Africa and South-east Asia are also rapidly urbanising, making them likely partners for infrastructure investment.

China appears to have leveraged African support in global arenas. For example, African governments comprised 25 of the 53 governments that signed a declaration supporting the Hong Kong National Security Law at the UN Human Rights Council.

Chinese involvement with Latin America and the Caribbean is less extensive but more worrying to Washington (see LATIN AMERICA/CHINA: Beijing's influence will grow - September 29, 2020). Some 20 countries have joined the BRI.

Washington worries too about Chinese-built ports on the Indian Ocean and rail links through mainland Southeast Asia, but the United States cannot rival China as a provider of infrastructure. Few US companies are interested in bidding on projects to build highways, railroads or ports; those that are, vastly prefer the domestic market.

Simply exhorting developing countries to beware of China does not address their vast infrastructure needs. At best, Washington can advocate on behalf of alternative partners, such as Japan and South Korea.

Beijing's efforts to reshape the world's transportation systems face other challenges, however. At home, China's economic woes from COVID-19 and US tariffs make it harder to justify spending overseas. Overseas, foreign governments are increasingly wary of 'debt traps'.

Interdependence and decoupling

Punitive tariffs, restrictions in the technology sector and the economic effects of the pandemic have contributed to dislocation on both sides. The 2020 US-China Business Council survey found that 86% of members believed trade tensions had damaged their business.

The economic impact of COVID-19 makes it impossible for either country to meet the targets in their 'phase one' trade agreement. These will need reassessment. Stabilisation is unlikely before the November 2020 elections, but will be a priority afterwards. China will resist negotiating additional 'phases' involving structural reforms.

> Despite growing distrust and antagonism, both governments recognise their economic interdependence

Both want to stabilise the trade relationship in the near term, but reduce the other's economic leverage in the long run by diversifying suppliers or developing indigenous substitutes.

The rest of the West

China's relations with Europe and Australasia largely lack military and great power rivalry elements, except inasmuch as these regions include key US allies.

China's priorities in these regions are economic advantage, ideological self-defence and diplomatic acquiescence on China's 'core interests' and politically sensitive issues.

Beijing cultivates ties with elites and uses economic incentives and coercion, with significant but decreasing success. A backlash is growing.

Europe

China sees Europe as declining and not a serious threat, except ideologically. Its priority for Europe is economic cooperation, all the more so amid escalating disputes with Washington.

The value China places on the EU's consumer market and high-tech manufactures will rise if China-US decoupling proceeds. This could facilitate a more assertive EU approach to China.

The EU's 2019 Strategic Outlook on China designated China as simultaneously:

- a cooperation partner on global issues;
- an economic competitor; and
- a "systemic rival" on issues of governance, including the uses of new technologies.

For China, Europe is principally an export market -- its largest if the EU is treated in aggregate. Europe is also potentially a valuable source of technology, brands and consumer demand as China attempts to move into high-end manufacturing.

> The most serious sources of bilateral tension are economic

Long-standing EU allegations of dumping and complaints about subsidies and lack of reciprocal market access have been joined more recently by concerns about growing competition in advanced industries.

Chinese investment in high-tech sectors and infrastructure, and Chinese exports of telecommunications technology, are increasingly politicised in Europe. Several countries and the EU as a whole have introduced investment screening mechanisms in recent years and, more recently, restricted use of Chinese telecoms equipment on national security grounds. 5G-related issues lie largely outside the EU's collective governance, making each country a diplomatic battleground.

China cultivates bilateral ties with individual EU members, such as Greece and Hungary, in order to shape and constrain the EU's collective stance. It has blocked some EU collective statements on human rights this way. Another potential fault line is Chinese engagement with Central-Eastern Europe through the '17+1' format and associated promises of greater connectivity via the BRI (see EUROPE/CHINA: Partners will reassess 17+1 forum - June 22, 2020).

Chinese warships occasionally held drills in the Mediterranean during the 2010s, including live-fire exercises, and joint exercises with Russia there and in the Baltic. UK and French warships have undertaken freedom of navigation in the South China Sea (see CHINA: New countries will challenge China sea claims - September 26, 2018).

However, Europe's security fears vis-a-vis China centre on cybersecurity, espionage and covert influence rather than military power.

China's prominence in the domestic politics of European countries is rising

Public opinion is generally unfriendly and becoming more so, reducing governments' latitude to work with China on the basis of economic interests alone (see EUROPE/CHINA: Public opinion is turning against China - July 28, 2020).

European Commission President Ursula von der Leyen announced plans last month for a 'European Magnitsky Act' that could put targeted sanctions on Chinese officials over human rights abuses (see INT/US: Global Magnitsky Act will extend sanctions - December 22, 2016).

Australia

China's primary interest in Australia is the country's high-quality iron ore. Beijing is doing little to advance the relationship beyond this. Political tensions and China's use of economic coercion in other sectors have not prevented the iron ore trade from growing.

China has attempted to punish Australia over its 'unfriendly' stances on issues such as political interference and human rights. It has frozen high-level political meetings since 2018. After Canberra called for an investigation into the origins of COVID-19, China halted beef imports from large Australian suppliers and put 'anti-dumping' taxes on Australian barley. Chinese government departments refuse to take calls from Australian ministers.

Beijing would welcome a weakening of the Australia-US alliance, but this is probably not a driver of its policy. China's routine designation of Australia as an 'unfriendly' country acknowledges that Australia's strategic posture is well-entrenched. Canberra intends to play a greater role in regional security affairs, as shown in its participation with India, Japan and the United States in the 'Quad' security partnership and its announcement in June of a AUD270bn (USD195bn) surge in defence spending over the next decade, including acquisition of long-range anti-ship missiles.

China for years sought to cultivate friendly political ties with Australian elites by fostering a sense of economic dependence, but opinion polls show a precipitous decline in Australians' opinions towards China since 2018.

The main influences on China policy in Australia are the national security agencies and some parliamentarians who are extremely wary of China. These constituencies tend to see bilateral tensions, declining economic cooperation and frozen people-to-people ties with China as beneficial for national security.

Canada’s military could face cuts after COVID-19

Wednesday, September 23, 2020

Canada’s government will need to plug the budget deficit post-COVID-19

Canada's flag displayed on military uniforms (Bumble Dee/Shutterstock)

Later today, Liberal Prime Minister Justin Trudeau’s government will reopen parliament with a speech detailing its updated objectives. This comes as COVID-19 has necessitated state support payments to Canadians, skewing the government’s budget and spending priorities. Canada’s military faces possible budget cuts at a time when Ottawa is attempting to modernise the military and maintain commitments to allies.

What next

Trudeau’s government is unlikely to reduce military spending immediately, as the armed forces are supporting the response to COVID-19. Yet Trudeau is probably eyeing an early election, perhaps in 2021. After that, to pay for spending priorities elsewhere, planned rises in defence spending could be cancelled and equipment purchases pushed back, hitting defence capacity for years to come. However, that would require that Trudeau is re-elected with a decent-sized majority.

Subsidiary Impacts

- Canada’s military will struggle to modernise its equipment, much of which is becoming outdated.
- Military recruitment and morale could be negatively affected by budget cuts.
- Further COVID-19 spikes would further strain Canada’s budget and increase its deficit.
- The military will be used to support the government’s COVID-19 management.

Analysis

COVID-19 has captured government policy this year. Ottawa has enacted fiscal and social aid packages for Canadians, which have knocked government spending and economic growth projections off course (see CANADA: Economic recovery from COVID-19 will take time - June 19, 2020 and see CANADA: COVID-19 is likely to force austerity - August 6, 2020).

The government now forecasts the budget deficit for the 2020/21 fiscal year at CAD343bn (USD255bn); CAD34bn was previously anticipated. Canada's 2020 defence budget is CAD22bn, 7.3% of the total budget.

Military and COVID-19

Canada's military has been crucial to the crisis response. It launched Operation Laser to protect military resources such as bases and support government counter-pandemic efforts. Canadian Rangers are deployed to rural and far-north towns to do everything from firefighting to chopping firewood. Soldiers were also deployed to nursing homes and were pivotal in drawing attention to care shortcomings in these institutions.

The Department of National Defense offered funding for research into COVID-19 solutions. Additionally, Canadanian forces deployed to support UN relief efforts, forming part of an airlift operation to Honduras, Trinidad and Tobago, Saint Vincent and the Grenadines, Guatemala and Barbados.

Canada's military is supporting the government's COVID-19 response

Equipment difficulties

Canada's military has only recently started to recover from post-Cold War defence cuts, where equipment was not replaced or modernised. Military spending fell from CAD12bn in 1993-94 to just over CAD9bn in 1998-99, the NATO Association said.

The consequences of cuts include extending the active life of military equipment by repairing and modifying it --, something still happening today.

With new funding programmed by former Prime Minister Paul Martin's Liberal government (2003-06) and enacted by Conservative former Prime Minister Stephen Harper's government (2006-15), budget cuts were reversed in 2006, after being stopped in 1999.

Strong, Secure and Engaged

In Trudeau's case, there is no guarantee military spending cuts will be announced in today's throne speech, especially as COVID-19 remains active and the military is needed to help. However, cuts or delays to some military spending and new projects could come as COVID-19 recedes, for instance if and when an effective vaccine is found.

Challenges could therefore lie ahead for the Strong, Secure and Engaged strategy -- the Trudeau government's military funding and modernisation plan initiated in mid-2017. The plan's aim is to increase defence spending to CAD33bn (USD25bn) in 2026-27, up from CAD19bn in 2016-17 and to modernise Canada's military for future challenges.

> Trudeau's government is trying to modernise the military and increase its funding

These challenges include dealing with natural disasters and similar emergencies. Another aim is to deepen defence ties with Washington and improve Canada's ability to take part in international peacekeeping operations. The plan also includes modernising and expanding the Canadian armed services and coast guard, and increasing the active military and reserves, to 71,500 and 30,000 people respectively.

The question is therefore timing. Trudeau is unlikely to slash spending when the military is helping tackle COVID-19. Any cuts or spending delays will probably come when they are affordable from the public health standpoint -- a COVID-19 vaccine is thought likely to become available during 2021 at the earliest.

Areas at risk?

In the long term, any military spending cuts are unlikely to be be as deep as those seen after the Cold War. Instead, they will amount to slowing the planned growth of the military budget. This will likely be done through cuts not to procurement but to activities such as transportation, operations and maintenance.

Yet there are some projects that are too advanced or too politically sensitive to cut. These include projects that are an employment lifeline in Canadian communities, such as shipbuilding, renovation and R&D in Halifax, Nova Scotia.

Electoral intervention?

The Trudeau government's speech today is likely the opening shot in calling an early federal election. Trudeau's government was returned as minority in 2019's election; the opposition Conservatives (now with a new leader, Erin O'Toole, installed this August) won the popular vote.

Trudeau's government won public praise for its handling of COVID-19, but the government then lost support after the WE charity scandal. Trudeau is unlikely to hold an election until COVID-19 is receding, but even then, there is no guarantee his government would be returned as a majority or at all.

If the Conservatives won the next election, they would probably be more sympathetic to protecting the military budget, while if Trudeau won a small majority or remained leader of a minority government, it would be easier for the Conservatives to pressure him to avoid cutting or moderating defence spending plans.

The US presidential election will also matter: if President Donald Trump is not re-elected, pressure on Washington's NATO allies, including Ottawa, to meet the 2% defence spending target for NATO members might reduce.

Longer-term considerations

While this context might be politically helpful in Ottawa in the short term, in the longer-term, Canada will need to increase its defence spending and military modernisation as competition for resources and influence develops in its neighbourhood, particularly the Artic and Greenland (see UNITED STATES: Attention will shift to the Arctic - July 22, 2020 and see UNITED STATES: Engagement in Greenland will intensify - July 15, 2020).

Meanwhile, if Trump is re-elected, he will likely maintain, if not increase, pressure on NATO allies to spend 2% of GDP on defence and buy US equipment; if Ottawa does reduce military spending, it could find itself provoking Trump's ire.

Another consideration relates to Canadian military recruitment and morale. Military spending cuts could reduce armed forces recruitment, something already proving problematic. Cuts could also undermine morale -- faulty equipment is already controversial, especially within the air force, which is currently trying to modernise an aircraft fleet that includes ageing fighters. The army and navy are also short of officers needed for key specialised positions.

A final concern is that Canada's military, like Germany's, has seen some rise in anti-government, far-right political feeling within its ranks in recent years. The Canadian Military Police said in 2020 that 16 serving individuals had been identified as members of hate groups, with another 35 committing "racist" or "hateful" behaviour.

This trend is likely to be accelerated by a backlash to government lockdown measures which has already manifested itself in small far right protests. Further budget cuts would worsen this trend.

Pandemic will test not topple authoritarian leaders

Monday, September 14, 2020

Authoritarian leaders face rising discontent over their mishandling of the pandemic-related health and economic crises

Anti-government protesters and students at a rally of the United Front of Thammasat and Demonstration group (Yuttachai Kongprasert/SOPA Images/Shutterstock)

Many authoritarian governments have taken advantage of the COVID-19 pandemic to expand their powers and tighten restrictions on opposition and civil society groups. Yet poor handling of the pandemic, combined with the prolonged economic downturn that has come in its wake, is testing their grip in states ranging from Belarus to Thailand and Zimbabwe.

What next

Long-standing authoritarian regimes are resilient and will attempt to co-opt and repress before relaxing their grip on power. Genuine democratic reform may be vetoed by regime hardliners and the security forces, for fear of prosecution for past abuses under a new dispensation. Democratic transition will, therefore, be limited to a small number of cases; many more will see further authoritarianism.

Subsidiary Impacts

- High-profile opposition and civil society mobilisation will draw greater attention to the repressive tactics of authoritarian states.

- The stress of the pandemic and divisions within the international community militate against foreign interventions for regime change.

- Prolonged economic slumps in large parts of Africa and Asia will fuel public anger against incompetent autocrats.

Analysis

The onset of the pandemic created new opportunities for authoritarian leaders to weaken institutional checks and balances:

- In Hungary, the government introduced a raft of new emergency powers with no sunset clause, undermining the role of parliament.
- In Uganda, the government used COVID-19 as a justification for banning opposition rallies in the run up to the 2021 general elections.

In many authoritarian states and fragile democracies, such restrictions have gone hand-in-hand with greater censorship as governments sought to stymie criticism of their response to the pandemic.

These developments strengthened the position of authoritarian leaders in the immediate run. However, the longer-term impacts of COVID-19 now threaten the grip of authoritarian governments -- and the magnitude of this challenge is only now becoming fully apparent (see AFRICA: COVID-19 and repression will fuel new protests - August 27, 2020).

The drivers of discontent

COVID-19 is the not the cause of public discontent with unpopular authoritarian regimes, which is rooted in a history of human rights abuses, poor public service delivery and unresponsive leadership. Rather, it has exacerbated popular frustrations.

The pandemic is fuelling public discontent against authoritarian leaders

Authoritarian blunders

While some authoritarian governments have been praised for early lockdowns, others have underplayed the health risk. This has especially undermined the confidence of urbanites -- who are more likely to contract the disease and to be able to access international coverage of its impact in other countries -- in the capacity and willingness of the government to respond to health emergencies.

In Belarus, for example, President Alexander Lukashenka’s reputation was damaged when he dismissed COVID-19 as a mass “psychosis” that could be treated with vodka. His folk-remedy approach added to other concerns that drove protesters onto the streets when he claimed victory in the August 9 presidential election.

Economic decline

All countries have suffered economically as a result of COVID-19, and the refusal of some authoritarian leaders to lock down their countries has meant that the impact of the pandemic on economic activity has been proportionally lower than in their democratic counterparts.

However, in poorly performing authoritarian states such as Lebanon, many citizens interpret economic hardship in light of the historic mismanagement of government revenue. As a result, governments struggle to persuade citizens that economic downturn is wholly attributable to COVID-19.

Moreover, the majority of authoritarian states already featured fragile economies and high levels of unemployment and debt prior to the pandemic. Zimbabwe, for example, was already in the middle of an economic crisis -- complete with hyperinflation and food shortages -- in early 2020.

Governments in these countries are poorly placed to manage the crisis with stimulus packages. This is especially true for countries that rely heavily on tourism for employment, such as Thailand, which is experiencing its worst economic contraction since the Asian financial crisis of 1998 -- and is projected to be one of the region's worst-performing economies this year.

Corruption

Corruption scandals both directly undermine public confidence in the regime and make it more likely that citizens will blame the government -- rather than the pandemic -- for economic hardship.

This is particularly true where corruption appears to have a direct impact on the official response to the pandemic. In Zimbabwe, Health Minister Obadiah Moyo was sacked and charged with abusing his office in relation to the improper awarding of a contract for COVID-19 supplies to a company that had allegedly inflated its prices. This intensified already growing public anger, contributing to anti-corruption protests at the end of July.

Outlook

Prolonged economic downturn will lead to increasing protests and demonstrations, but as the recent transition in Sudan demonstrates, this is unlikely to lead to the downfall of the government unless there is a split within the regime itself. Unless a faction of the government and the security forces decide to support -- or at the very least allow -- political change, rising discontent is likely to result in heightened repression.

Belarus

Sustained mass protests following the presidential election have been met with a heavy-handed riot police response. This has failed to intimidate the crowds, whose main demand is Lukashenka's resignation.

Lukashenka has the security forces on his side and the constitution reform he is offering is not intended to weaken his position.

The EU is threatening sanctions but is treading carefully to avoid giving Moscow a pretext for intervention. President Vladimir Putin is seeing Lukashenka today, and is considering the best way forward, which probably involves keeping him in place in the short term, extracting economic and political concessions from him and eventually easing him out in favour of a more manageable Kremlin client (see BELARUS: Country in flux as Moscow weighs options - August 25, 2020)).

Thailand

Despite a coronavirus ban on large gatherings, thousands of young people joined anti-government protests in early August, after students publicly questioned the role of the royal family, despite the country's strict lese majeste laws.

Prayuth's government will allow protests -- for now

The protesters have three main demands that are all related to the close relationship between the royal family, the military and the nominally civilian government of Prime Minister Prayuth Chan-ocha -- and the decision to prohibit the pro-democracy Future Forward Party (FFP) in February.

Protesters want:

- parliament to be dissolved;
- the constitution to be rewritten; and
- the authorities to stop harassing critics.

However, while the protests were the largest the capital has seen in years, they do not appear to be on a scale that could force the political-royal-military alliance to relinquish its hold on power in the near future (see THAILAND: Protests will bring protracted instability - August 24, 2020).

Zimbabwe

President Emmerson Mnangagwa has responded to mounting criticism of his regime by shutting down urban areas to prevent mass demonstrations and arresting prominent journalists and dissidents such as Hopewell Chin'ono -- despite social media criticism.

Chin'ono and opposition leader Jacob Ngarivhume were belatedly released on jail following a build-up of international pressure but remain on trial. South African-attempted mediation has so far been ineffective.

The military depends on access to power to sustain its control over key sectors of the economy and so is likely to either demand that Mnangagwa stays in power or determine his successor. A prominent military figure such as Vice-President Constantino Chiwenga (health depending) is most likely to be promoted.

Either eventuality would serve to sustain the status quo, while the transfer of power to Chiwenga would most probably lead to a further militarisation of the state, reducing the prospects for free and fair elections (see ZIMBABWE: ZANU-PF may face renewed leadership upheaval - June 11, 2020).