An Oxford Analytica Briefing Book

Cybersecurity & Geopolitics

Curated for guests of the Glasswall Cyber Dinner

London – March 26, 2018

Oxford Analytica

GLASSWALL™
TRUST EVERY FILE

CONTENTS

Foreword

Oxford Analytica is delighted to provide this background Briefing Book for guests of the Glasswall Cyber Dinner

David R. Young
Founder and President
Oxford Analytica

We have curated analyses from the Oxford Analytica Daily Brief to showcase some of the critical trends and geographies that lie at the intersection of cyber and geopolitics in the contiguous domains of cyberwarfare, security and crime.

These range from how North Korea uses cybertheft to evade international sanctions to how Russia and NATO are institutionalising cyber commands to improve their capacity to wage information, hybrid and asymmetric warfare and how China is at the forefront of global advances in quantum cryptography and communications that will transform cybersecurity.

Oxford Analytica is an international consulting firm founded in 1975 to enable governments, corporations and international organisations navigate the intricate macro environments that impact their strategies, operations, investments and policies.

We do so by drawing on a network of some 1,500 experts at leading centres of learning around the world who can bring clarity to the complexity of global events and thus deliver insight that can be incorporated directly into our client's work.

The firm's worldwide reputation for delivering unparalleled, authoritative and impartial macro diligence is based on our founding principles, robust methodologies and an impressive track record.

If you have any questions arising from the articles that follow or on any of the services we provide, please do not hesitate to contact me.

Yours sincerely,

David R. Young,
Founder and President
Oxford Analytica

Prospects for cybersecurity in 2018

Wednesday, November 29, 2017

High profile cyberattacks, leaks and disinformation campaigns in 2017 have elevated the importance of cybersecurity

A computer hacker tries to access information in a Voting Machine Hacking Village during the Def Con hacker convention in Nevada, US, July 2017 (Reuters/Steve Marcus)

Business leaders and government officials now realise that cybersecurity is a key strategic issue -- one that can threaten an organisation's reputation or even undermine a state's political process. However, although leaders might acknowledge the growing importance of the issue, few understand how to proceed. 2018 will therefore be characterised as a time of adaptation. A key priority will be to build more cohesive organisations, with active and streamlined communication from the IT department to the executive level.

What next

Many governments have historically been latecomers to cybersecurity issues, but 2018 will see them becoming increasingly assertive. This emergence of state actors will be most clearly felt at the European level where tighter regulation will be introduced that will significantly affect businesses. Organisations will also become more open about cybersecurity, both because of new regulations and also because lessons in press relations from previous data breaches show that organisations are better off getting ahead of the narrative by being proactive in their communications with the media and their customers.

Strategic summary

- With leaks and disinformation campaigns growing in prominence, the cybersecurity of data will become an important issue for political parties.
- The global cybersecurity skill shortage makes recruitment a significant challenge.
- The high profile of ransomware incidents will pique the interest of hackers who will see the method as a way to capture attention and money.

Analysis

The digital domain has traditionally been dominated by technology firms and the private sector, but 2018 will see a shift in the nexus of power. Governments are set to intervene further in the market regarding cybersecurity issues. Already they focus on legislating against 'fake news' and disinformation campaigns (see INTERNATIONAL: 'Fake news' fight focuses on internet - March 22, 2017).

Businesses can expect increased exposure to government fines and will simultaneously also see the burden of responsibility and legal liability regarding cyberattacks shift towards them.

Regulation on how to manage cybersecurity incidents is set to increase

This is most clearly seen in an EU context through the General Data Protection Regulation (GDPR) that comes into force in May 2018. The GDPR encompasses various issues including privacy and the storage of personal data. It will require businesses to notify both customers and the authorities about data breaches.

The regulation will also increase the obligation of businesses to follow established cybersecurity practices and will impose significant fines for non-compliance: an egregious violation of GDPR rules

could result in a fine up to either 20 million euros (23.7 million dollars) or 4% of annual revenue (whichever is highest). It will be the national supervisory authorities (or the lead authority in an investigation) that will determine the sanction.

Although it is unlikely that the authorities will immediately begin to impose the maximum fine, it does nonetheless mean that cybersecurity is now a key component of a business's risk management strategy. For UK businesses hoping to escape such regulation in the context of Brexit, UK Digital Minister Matt Hancock has confirmed that the United Kingdom will replace the 1988 Data Protection Act with legislation that mirrors the GDPR (see PROSPECTS 2018: Internet governance - November 9, 2017).

Data breaches

Cyberattacks and data breaches now frequently occupy headline news. The increased coverage of cyberattacks comes with greater risks for organisations. On November 21, Uber announced that it had failed to disclose information regarding a data breach in 2016 that affected 57 million users' accounts. The incident put a dent in the firm's attempt to restore its reputation. Following the hacking scandal, a group of investors offered to buy shares at Uber at a company valuation of 48 billion dollars, down 30% from its last fundraising valuation of 69 billion dollars. Investigations of the company are also due to start.

> Data breaches have a severe effect on firms' reputations

Cybersecurity negligence increasingly has legal implications: after suffering a data breach in mid-2017, Equifax is now faced with a class-action lawsuit that could see the firm pay over 1 billion dollars to consumers who had their personal data and social security numbers stolen. The response to the greater significance of cybersecurity will be an elevation of the issue at the board and c-suite level. Although this process is already underway, 2018 will see chief information security officers play a more important role while chief executive officers will have to acknowledge the importance of cybersecurity through leading by example.

Cybersecurity will also rise in prominence at the political level. The US government, for example, was highly vocal in its condemnation of Russian-based antivirus firm Kaspersky, stating that the firm could not be trusted after it was alleged that Kaspersky worked closely with the Russian government to spy on US personnel. The interactions of technology firms with governments are likely to be further scrutinised next year -- a process that has received significant attention ever since former US National Security Agency (NSA) contractor Edward Snowden outlined the relationship between the US government and US-based technology firms.

The actions of governments will also be further examined. With the WannaCry ransomware that spread globally using leaked NSA tools, there will be further questions surrounding how government agencies store and secure the cyber tools they possess that could have damaging effects (see INTERNATIONAL:Vulnerability disclosure deeply divides - May 25, 2017). The US government in mid-November established a clearer and more transparent process for how cyber vulnerabilities will be managed and other states will likely follow suit.

Likewise, given the politically damaging nature of leaks (as seen most clearly in the 2016 US presidential election), governments and political parties will increasingly regard safeguarding their data as a key component of a winning election strategy.

Threat surface

The majority of cyberattacks in 2018 will be on the back of tried and tested hacking techniques. A significant proportion of incidents will continue to use known vulnerabilities. For organisations, this means that there is a lot in their power to prevent cyberattacks. Implementing simple cyber hygiene measures -- such as regularly patching software, maintaining clear access controls and implementing properly functioning firewalls -- will go a long way in bolstering an organisation's security.

Likewise, given the global profile of the WannaCry ransomware that infected systems across the world, including over 40 National Health Service (NHS) hospitals in the United Kingdom, it is likely that hackers will continue to exploit this technique and demand ransoms (see INTERNATIONAL: Ransomware fight will be uphill battle - May 15, 2017). Crucially, as organisations agree to pay ransoms to hackers (either through ransomware or in cyber incident contexts) the incentives for other hackers to launch similar initiatives will increase.

Security concerns related to the increase in connected everyday devices (known as the internet of things -- IoT) will intensify next year. As more devices are connected online, from smart watches to fridges, the total number of attack vectors is increasing. Many of these devices are sold at a low price, making it doubtful that their economic model will support the prioritisation of security (see INTERNATIONAL: Hackers will use the Internet of Things - October 24, 2016).

Shifts in the labour market

There is a well-documented global shortage of cybersecurity professionals -- a trend likely to be sustained in the medium term. The skill shortage has traditionally been mentioned in reference to the lack of those with technical skills in topics including software engineering, penetration testing and forensic analysis.

However, this will increasingly also encompass a variety of other skill sets with an increased awareness that disciplines such as psychology, risk management and law all have a clear application to cybersecurity.

Given the importance of a wider set of skills and insights, there will be an even more acute need for people who can cross between different thought silos -- perhaps, for example, people who can understand the highly technical challenges faced by a security team, before distilling their strategic implications and articulating them clearly to executives.

Organisations will be faced with three options:

- they can offer highly competitive salaries at or even above the going market rate;
- they can outsource aspects of their cybersecurity -- this is a popular model at the moment and allows specialist cybersecurity teams and consultancies to serve a variety of clients simultaneously; or
- they can hire people with related skills (such as a core understanding of computer science) and train them up in more specific skills related to cybersecurity.

For the majority of organisations, aspects of all three of these strategies are likely to apply.

Despite the broader shortage of cybersecurity skills, there is some room for optimism. Although women have been chronically underrepresented in the cybersecurity industry, the future outlook appears positive. A combination of professional and educational initiatives have specifically sought to get more women into the industry. The UK National Cybersecurity Centre in February 2017 launched a 'girls only' cyber competition, for example, providing a clear pathway into the profession. Some of these sorts of initiatives have now been in place for a few years; 2018 should see a more diverse talent pool, with the prospects in the medium-to-long term even brighter.

North Korean cybertheft will grow as sanctions bite

Wednesday, March 14, 2018

Businesses are coming under attack by a nation-state desperate for currency


North Korean flag (Reuters/Denis Balibouse)

Hacker groups linked to North Korea are believed to be behind some of the world's most aggressive cyberattacks. They are a potential threat to many organisations -- public, private and non-profit alike.

What next

With North Korea's economy on course to suffer serious damage from economic sanctions, Pyongyang will rely more on cybercrime as a source of currency. Other states will struggle to develop and implement doctrines to deter such activity. North Korea will exploit this confusion.

Subsidiary Impacts

- States where North Korean hacking cells are located will come under pressure from victim states to eliminate them.
- Revenue-seeking North Korean cybercrime will target cryptocurrency holders and large financial institutions.
- States that are victims of North Korea cyberattacks will likely respond via non-cyber means, such as economic sanctions.

Analysis

North Korea's military is believed to have had cyber operations since at least 1998.

The country's offensive cyber capabilities are not on par with those of the United States, Russia and China, but they are significant. Attacks attributed to North Korea have caused considerable disruption since at least 2009, particularly in South Korea.

North Korean hackers have used 'social engineering' tactics, using deception to manipulate individuals into providing data or login credentials.

They have also carried out complex multi-stage attacks. For example, they have used cryptocurrency-related lures initially to infect victims with reconnaissance malware and backdoors, before then infecting targets of interest with additional malware to steal credentials for cryptocurrency wallets and exchanges.

Aims and intentions

As with most states, North Korea's cyber operations reflect Pyongyang's strategic and geopolitical interests. South Korean targets -- both government and private -- were the initial focus of North Korean cyberattacks in the 2000s.

Attacks attributed to North Korea since then include:

- a series of attacks in rapid succession in 2013 on South Korean banks, broadcasters and NGOs hostile to the North Korean regime (see NORTH KOREA: Hacking offers Pyongyang low-risk weapon - April 11, 2013);
- the theft of nuclear power plant designs from South Korea's state-owned nuclear power company in 2014 (see SOUTH KOREA: Cyber attacks threaten nuclear safety - January 7, 2015);
- an attack on Sony Pictures in the United States in 2014 after the film studio was set to release 'The Interview', a satirical comedy that depicted the assassination of North Korea's supreme leader Kim Jong-un (see NORTH KOREA: Cyber attacks exploit fundamental flaws - December

18, 2014); and
- the theft of joint South Korea-US war plans in 2016 (see NORTH KOREA: Hacking endangers South Korean security - October 10, 2017).

In 2017, a group linked to North Korea was associated with six campaigns that overwhelmingly targeted South Korean users specifically and used phishing emails referring to Korean reunification and human rights in North Korea.

Financial motive

Most states deploy cyber capabilities for espionage or offensive purposes. North Korea is unusual in that many of its cyberattacks seek financial gain -- an urgent priority for the heavily sanctioned government of an impoverished country.

These revenue-generating aspects of North Korean operations were well publicised in 2016 when North Korean hackers attempted to transfer 950 million dollars from Bangladesh's central bank using the SWIFT secure messaging system. Although most of the transfer was forestalled, 81 million dollars disappeared.

The North Korean government also has established cells that make money through more banal means, such as hacking gambling sites and creating bots that make money through online games. Such activities offer smaller rewards, but require a less sophisticated skill set and are likely to provide a reasonably consistent stream of income.

North Korea has for decades used its diplomatic missions to earn foreign currency by smuggling narcotics, alcohol, cigarettes and ivory (see NORTH KOREA: Sanctions target illegal embassy trade - May 20, 2013). Cybercrime is a more attractive alternative.

Cryptocurrencies

North Korea has targeted bitcoin and other cryptocurrencies. Having lured victims interested in bitcoin with sophisticated malware, North Korean hackers then steal credentials for cryptocurrency wallets and exchanges.

North Korean hackers demanded payment in bitcoin from victims of the WannaCry ransomware last year. That attack crippled computer systems across the globe but was not particularly profitable, earning its perpetrators just 150,000 dollars.

Offshore hacking

North Korean hacker units are located across Asia, including in China, South Korea and Malaysia. Finding them has proved difficult.

> North Korea is unusual in placing hacker groups abroad

Two things explain this strategy.

First, sending hackers abroad represents a wartime contingency plan. If North Korea were under attack, its hacker groups would still be able to operate, ensuring the survival of what is becoming an increasingly important strategic asset.

Second, such a disparate model helps to mask the identities of North Korean hackers. There is minimal internet access in North Korea, which makes it easier for intelligence agencies to track internet traffic going in and out. North Korean hackers based overseas can more easily hide their identities and intentions. A North Korean hacker group based in China or South Korea could be confused for a domestic hacker group or criminal organisation.

Domain asymmetry

Possessing advanced technology is usually a strategic advantage for states, but from a cybersecurity perspective, it is a double-edged sword: the states that depend most on advanced technology are the most vulnerable when that technology is compromised.

> North Korea is a striking example of the fundamental asymmetry in the cyber domain

In South Korea, the ubiquity of technology and connected devices creates a broad attack surface.

For North Korea, however, the decision to restrict internet access and related technology makes the state and the national economy significantly less vulnerable to cyberattacks.

Therefore, even though North Korea is highly aggressive in its cyberattacks, Pyongyang's targets cannot easily retaliate in kind.

The difficulty of attributing a cyberattack further complicates retaliation. North Korea has always denied responsibility. The evidence is not always conclusive.

This will prompt target states to retaliate via other means, as when Washington imposed sanctions on North Korea following the Sony Pictures hack.

What constitutes proportionate retaliation is not easily established. In a worst-case scenario, a North Korean cyberattack that caused fatalities or widespread economic disruption could ultimately escalate to physical conflict (see NORTH KOREA: Risk of war will grow if trends continue - August 9, 2017).

North Korea is not wholly immune to cyberattack and Washington, in particular, will exploit what vulnerabilities it does have to disrupt its nuclear weapons programme, as it did with Stuxnet in Iran.

Russia will deny cyberattacks despite more US evidence

Tuesday, February 20, 2018

The US authorities are setting out stronger evidence of Russian interference


Special Counsel Robert Mueller (Reuters/Aaron P. Bernstein)

Russian Foreign Minister Sergey Lavrov yesterday dismissed the 'lack of evidence' in the indictment issued against alleged Russian 'trolls' at the request of Robert Mueller, the US special counsel investigating interference in the 2016 presidential election. The US indictment accuses the St Petersburg-based Internet Research Agency, its backers and staff of interfering in the election by running false social media accounts. This account of Russian trolling comes soon after US and UK accusations of Kremlin responsibility for a June 2017 cyberattack that disrupted computer systems in Ukraine and elsewhere.

What next

The revelations will hamper efforts to form a US-Russian working group to develop cybersecurity norms. Moscow will respond to US claims with flat denials and the development of more sophisticated capabilities to evade detection. Greater awareness of hacker groups' mixed criminal and political activities may help investigators track them.

Subsidiary Impacts

- Private sector firms will play a growing role in attributing state-sponsored cyber attacks.
- Governments will become increasingly reliant on private sector capabilities, whose distance can save them diplomatic embarrassment.
- 'Exploits' made public could be used in hostile cyber operations.

Analysis

Officials in Moscow deny or laugh off allegations of Russian cyberwarfare and 'false flag' social media activity. This line of defence is helped by the difficulty of definitive attribution, and by the authorities' practice of farming out both kinds of activities to non-state actors. This gave President Vladimir Putin scope to shift from absolute denial to an admission in June 2017 that freelance hackers might have taken action against opponents of Russia, without Kremlin knowledge or approval (see RUSSIA/US: 'Freelance' hack claim to blunt US probe - June 2, 2017).

The argument that Western allegations lack substance is becoming harder to sustain as US statements on cyberattacks get tougher and the Mueller investigation digs up evidence. The indictment of the Internet Research Agency is likely to be only one of many lines of investigation.

'Troll factory' indictment

The name, address and activities of the Internet Research Agency have been public knowledge for more than a year, making it the worst kept secret of Russian covert operations (see RUSSIA: People may be persuaded by hacking revelations - October 17, 2017).

The February 16 indictment issued by a federal grand jury in Washington, DC put specific names to the agency's staff and outlines its organisational and funding arrangements:

- Businessman Yevgeny Prigozhin and two companies he controls are said to have funded the Internet Research Agency; Prigozhin is already on the US sanctions list (see RUSSIA/SYRIA: Deal-making - June 27, 2017);
- Staff members set up social media accounts using fake identities to conduct a campaign that included supporting Donald Trump's candidacy for the US presidency in 2016 and disparaging Democratic candidate Hillary Clinton, as well as attempting to suppress potential Clinton vote among ethnic minorities.

- The campaign also involved purchases of online advertisements and the orchestration of political rallies on spurious themes in the United States.

The Internet Research Agency is also suspected of interfering in other electoral processes, and UK politicians are taking a hard look at alleged social media meddling in the Brexit campaign (see RUSSIA/UK: 'Trolls' get more attention - December 7, 2017).

Cyberwarfare

February 15 statements from the White House and the UK Foreign Office blame Russia directly for the June 2017 'NotPetya' cyberattack on Ukraine and other states. The US statement cited the Russian military as the perpetrator, implying involvement of the armed forces' intelligence service, the Main Intelligence Directorate (GRU).

The NotPetya incident initially affected Ukrainian accounting software but spread to become one of the most serious cyber attacks of 2017, hitting banks, energy companies, government offices and an airport in countries including India, the United States and Russia itself.

In just one of many impacts, Maersk, the world's largest shipping company, had to install 4,000 new servers and 45,000 computers at a cost of 250-300 million dollars.

> NotPetya looked like a ransomware attack but this may have been a disguise

The cyberattack looked initially like a ransomware operation, where users find their data locked with a message to pay money in exchange for decryption. This made it look as though the perpetrators were criminals with no political affiliation or motivation.

Cyber experts at the UK National Cyber Security Centre believe the GRU was almost certainly responsible for the NotPetya attack. The same conclusion was drawn by the CIA with "high confidence" in November.

State, non-state or quasi-state

The Russian intelligence services are believed to contract out much of their cyber activities to a range of hacker groups.

The unorthodox nature of these contacts was illustrated with the arrest last year of Sergey Mikhailov and Dmitry Dokuchayev, officers with the Federal Security Service (FSB) employed in its elite Information Security Centre.

The arrests were reportedly conducted because the authorities believed US intelligence was being tipped off about Russian cyber operations by individuals with access to classified information. Both suspects were also reported to have overseen Shaltay-Boltay (Humpty Dumpty), a hacker group that blackmailed prominent Russians for profit rather than political ends (see RUSSIA: Arrests unlikely to derail cyberespionage - February 21, 2017).

Ukraine

Because of the ongoing conflict, Ukraine has repeatedly been targeted by hacker groups of Russian origin. Some see Ukraine as a testing ground for various methodologies -- perhaps even as a 'showcase' to demonstrate to the West what Russia is capable of.

The IT security company ESET suggested that a Russia-based hacker group called Sandworm (also known as TeleBots) carried out the NotPetya attack. Sandworm cut off power to hundreds of thousands of people in 2015 and 2016 through attacks on Ukrainian electric utilities.

Another group called CyberBerkut uses cyber attacks to discredit the Kyiv government. Researchers from the Citizen Lab have found links between CyberBerkut and the FancyBear group.

US election hacking

Fancy Bear (also known as Sofancy or APT 28) and Cozy Bear (also known as APT 29 or FancyDuke) came to public attention after being identified as having broken into US Democratic National Committee (DNC) computer networks ahead of the 2016 election.

Fancy Bear is thought to be controlled by the GRU, while Cozy Bear is linked to the FSB.

Crowdstrike, the firm which discovered the DNC intrusion, stated that the intrusions occurred at different times and the perpetrators appeared unaware of one another's actions. This points to adversarial relations between the GRU and the FSB, a domestic intelligence agency with no remit to operate abroad. Tracking inter-agency rivalries may help Western governments discover weaknesses and predict the nature of future attacks.

> Russian intelligence agencies run separate rather than coordinated operations

Konstantin Kozlovsky, put on trial in Russia last year for alleged membership of a bank-hacking crime group, testified in December that he had been hired by the FSB to access DNC networks. While this has not been confirmed by the DNC or Crowdstrike, Kozlovsky claims he left a data signature in the DNC's servers to prove his involvement.

Reports recently surfaced indicating that the Dutch intelligence service penetrated Cozy Bear networks as long ago as 2014, tracked the group's activities and shared intelligence on DNC data theft with its US counterparts.

Shadow Brokers

The Shadow Brokers are one of the most mysterious hacker groups believed to be associated with Russia, and have since 2016 published hacking tools and computer exploits stolen from Equation Group, an elite hacking unit of the US National Security Agency (NSA).

The Shadow Brokers leaked an exploit associated with the NSA, called EternalBlue, in early 2017. This exploit has since been used in a number of ransomware operations, including by the authors of WannaCry, which targeted the UK National Health Service in May 2017 (see INTERNATIONAL:Vulnerability disclosure deeply divides - May 25, 2017).

Gulf split heralds new uses for cyber capabilities

Tuesday, February 6, 2018

Regional tensions among Gulf Arab countries highlight the increasing salience of the online world


A staff member at Qatar News Agency in Doha (Reuters/Tom Finn)

Gulf social media are today involved in a battle of hashtags over an alleged Qatari call to 'internationalise' the holy sites in Saudi Arabia's Mecca and Medina -- a call Doha says it never made. The Qatar crisis in June 2017 was similarly sparked by a piece of 'fake news' planted on Doha's national news agency showing the Qatari emir as expressing support for Iran and the Muslim Brotherhood movement. The incidents are part of a rising trend of offensive cyber actions and government-backed social media contestation in the region. They may also be the first examples of a combined cyber and physical strategy achieving core foreign policy goals just short of actual conflict.

What next

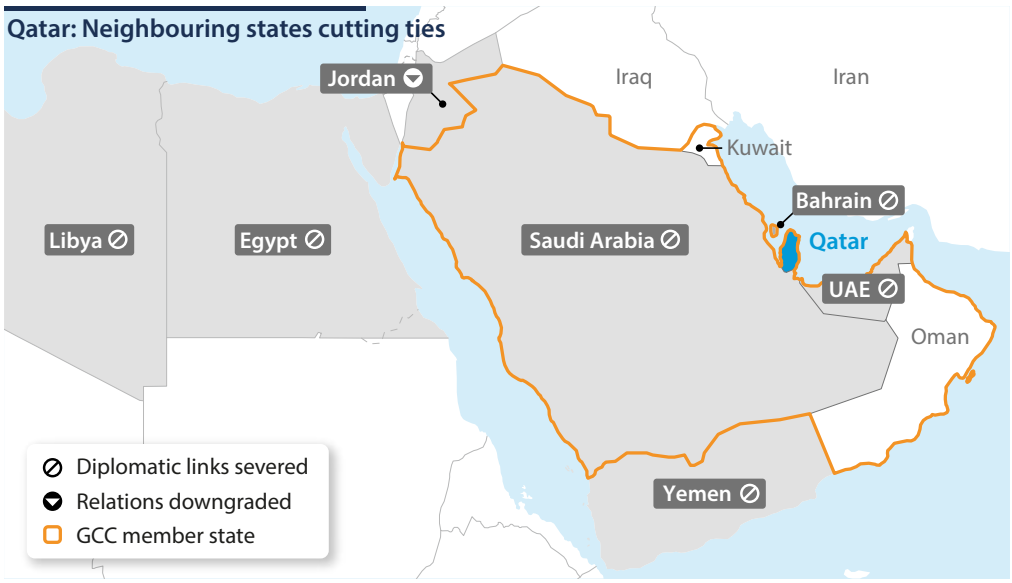
Some Gulf Cooperation Council (GCC) countries will increasingly use cyber operations to achieve geopolitical ends, as do other highly connected states. However, like their main ally Washington and their major adversary Tehran, they will seek to keep such actions from triggering actual conflict by maintaining ambiguity of attribution. Contractors will generally be used for these operations, due to their deniability and relatively low costs, but their use could create political and reputation risks through leaks and conflicts of interests.

Subsidiary Impacts

- The GCC's high online presence and draconian regulatory framework will make social media a key arena for covert state action.
- Interpretation of past events will fragment, meaning divisions such as the GCC split harden over time and become difficult to reverse.
- As GCC states' attitudes to Iran diverge further, their Western allies will find regional diplomacy more labour-intensive.

Analysis

Saudi Arabia, the United Arab Emirates (UAE), Egypt and Bahrain ('the quartet') on June 5, 2017 launched a political and economic boycott of Qatar: recalling citizens, withdrawing ambassadors and cutting land, air and sea links (see QATAR: Arab enemies may impose new sanctions - June 26, 2017).



The boycott was the culmination of a long cycle of dispute and reconciliation between Qatar and its neighbours. Its general justification was Qatar's support for 'terrorism', defined broadly to include backing for opposition groups elsewhere in the region, such as the Muslim Brotherhood, through such tools as Doha's Al Jazeera television channel (see QATAR: Doha will deploy Al Jazeera as a vital weapon - October 23, 2017). However, closer triggers included:

- the increasingly close alignment between activist Saudi Crown Prince Mohammed bin Salman and the crown prince of Abu Dhabi, Mohammed bin Zayed, who has long opposed Qatar's links with the Muslim Brotherhood; and
- the apparent backing, in his visit to Riyadh in May, of US President Donald Trump, who tweeted his support for the quartet the day after the boycott -- although this was later contradicted by the neutral stance of other US government departments and replaced by an offer of mediation.

Cyber instigation

The immediate pretext for the quartet's actions was footage of the Qatari emir that appeared on the website of Qatar News Agency (QNA) just after midnight on May 24, 2017, with text that portrayed him as expressing support for Iran and the Muslim Brotherhood.

Following its publication, news agencies in the quartet countries picked up the story almost immediately, resulting in claims that they were prepared for or tipped off about its release. At least three dailies in Saudi Arabia and one in UAE led with it in their morning headlines on May 24.

Anonymous sources blamed Qatar's Gulf rivals

Qatar's investigation, which was supported by the FBI and the UK National Crime Agency, concluded that the appearance of the video was the result of a hostile cyber operation against QNA. Sources told the international press that the UAE or Saudi Arabia hired Russian contractors to conduct the operation.

The Washington Post reported unnamed US national security officials as saying that the intrusion was carried out by contractors working for Abu Dhabi. Separately, The New York Times cited anonymous US and Qatari officials as blaming Russian hackers for hire, and the Guardian reported observers' suggestions that the UAE or Saudi Arabia had commissioned the hackers.

In addition, the Qatari attorney-general on June 20 claimed Doha had evidence that iPhones from the quartet countries were used in the operation. Nevertheless, the attribution of cyber operations is extremely difficult, and the forensic analysis is not publicly available (see INTERNATIONAL: Impunity will incentivise cyberattacks - December 16, 2016).

GCC cyber warfare

The QNA cyber operation follows a wider pattern of cyber tools deployed to achieve largely domestic policy and security objectives in Egypt and the GCC states. All these countries, including Qatar, have invested heavily in technologies for large-scale and targeted surveillance manufactured by companies in the United States, Europe and -- in the case of the UAE -- Israel.

> Surveillance against activists can be a bridge to offensive operations

Possession of surveillance technologies (which is mostly outsourced) has usually been revealed after their use against dissidents and activists. However, these technologies are also linked to offensive cyber activity, involving the active penetration of an adversary's networks (which would likely be carried out by the GCC and Egyptian governments themselves).

Governments in the region benefit from buying offensive cyber technologies not only through deploying the technologies themselves, but also by learning and replicating them. In addition, they develop close working relationships with cyber contractors.

Other cyber tools were also used during the Qatar crisis. The site 'Qatarileaks' was created at around the same time, carrying anti-Qatar propaganda.

Just before the ostracisation, but after the QNA incident, an unknown individual offered the private emails of the influential UAE ambassador to Washington, Yusuf al-Otaiba, to several US news outlets. These emails indicated that Otaiba had significant influence with several think tanks and government figures including Jared Kushner, as well as a lavish lifestyle and anti-Qatar posture. Their publication was probably a Qatari response to the earlier cyber operation.

Social media aspects

Both sides also recognised the importance of social media in shaping public opinion in their favour. Immediately after the boycott, the UAE attorney-general defined showing sympathy for Qatar online as a cybercrime, resulting in prison sentences between 3-15 years.

This announcement highlights the fact that all the GCC countries have broad definitions of 'cybercrime' and harsh punishments for online speech relative to international norms (see UNITED ARAB EMIRATES: Government will monitor internet - December 15, 2016).

This social media antagonism has continued. Throughout August, a popular Saudi figure on Twitter misleadingly interpreted the quantity of anti-Qatar hashtags as demonstrating popular support against the ruling Al Thani family in Qatar, even though most of those accounts were located in Saudi Arabia. In December, the popular 'Saudi citizen' account was hijacked, tweeting pro-Al Thani comments.

New strategic model?

However, unlike the QNA operation, these actions were not accompanied by a wider political strategy. Uniquely, the fake video was part of a coordinated strategy involving media coverage and immediate policy 'reaction'.

Despite Qatar's immediate denials and later evidence of tampering, this strategy was successful in isolating Qatar. Key factors included control of the press and social media, and the tactic of doubling-down on the accusations -- for example, by releasing a list of demands.

This new form of cyber action is more tightly directed than Russian disinformation campaigns against European elections, and more clearly part of a foreign policy strategy than the Russian cyber operations against Estonia were a decade ago. It is also more overt than the 'effects' operations undertaken by US and UK intelligence agencies (which, for example, set up false online identities and resources).

Although the United States has used joint cyber-physical operations successfully against Islamic State in Syria, such joint operations are rare outside war contexts. This is therefore the first example of a combined cyber and physical strategy achieving core foreign policy goals just short of actual conflict. It may be used more frequently in future disputes.

New commands will support NATO's European focus

Monday, February 5, 2018

NATO is turning greater attention towards the European theatre

NATO Cooperative Cyber Defence Centre of Excellence, Estonian and NATO flags are seen in front of member countries' flags at the centre premises in Tallinn, Estonia (Reuters/Ints Kalnins)

In July, NATO is expected formally to adopt a new command structure at its summit in Brussels. Two new commands, focusing on the North Atlantic and on logistics, plus a cyber operations centre, will be created. NATO is adapting to the new security environment in Europe and returning to a larger command structure and in-area rather than out-of-area crisis management efforts.

What next

Once established, the new commands are likely initially to be small in size and scope, but they could grow in stature and responsibility in coming years. This will depend on the future trajectory of the security situation in and around Europe. Internal discussions are underway within the Alliance on where to locate the new commands; Germany will probably gain the logistics command, and the US state of Virginia the Atlantic command at Norfolk.

Subsidiary Impacts

- Much of NATO's attention will be on Russian defence and military moves near Europe.
- The two commands will strengthen NATO's ability efficiently to move assets about, and to engage in cyber activities.
- Other commands could be created in coming years, such as for the Baltic Sea and Black Sea regions.
- NATO's Southern Hub in Italy could be further developed to focus on North Africa and the Middle East.
- Other commands could close or be downsized, such as the UK-based Maritime Command and US-based Allied Command Transformation.

Analysis

The coming of the two new commands and cyber operations centre follows three years of NATO adapting to the new European security environment, given Russian assertiveness following the annexation of part of Ukraine and now the continuing political and security turbulence in North Africa and the Middle East.

> NATO is responding to changes in the European security environment

Since 2014, NATO has among other things created a forward presence in Poland, the Baltic States and Romania (see EASTERN EUROPE: Russian navy raises Black Sea tensions - June 16, 2017 and see BALKANS/NATO: Perceived threat will set defence spend - June 6, 2017).

It has also increased the size and scope of Alliance exercises in Eastern Europe and made contributions to the campaign to defeat Islamic State in Iraq and Syria. The new commands are a logical next step in putting NATO's adaptation onto a long-term footing.

Atlantic Command

The vulnerability of the North Atlantic sea lanes has risen in prominence within NATO over the last two years.

NATO's ability to deter and defend against Russian aggression aimed at the Alliance's eastern members relies on the ability quickly to flow reinforcements, and particularly US forces coming across the Atlantic Ocean, to north-east Europe and elsewhere.

Yet this capability has been questioned, given the Russian navy's resurgence. In particular, Russia's submarine force is increasingly sophisticated and can leverage new weapons such as long-range anti-ship and land-attack cruise missiles.

Following the Cold War, NATO's command structure dedicated to the North Atlantic and intra-Europe operations was disassembled in favour of a streamlined structure dedicated to supporting operations outside NATO's area. These ranged from the Balkans to Afghanistan and the Horn of Africa.

The envisioned Atlantic Command would begin to return NATO to its North Atlantic focus and would be dedicated to developing and running exercises and monitoring the North Atlantic maritime domain in peacetime and assuring the access of Europe across the North Atlantic in wartime.

The United States is likely to serve as the host nation for the new Atlantic Command, a role it held in the Cold War. It already has much of the necessary infrastructure and command and control arrangements. Additionally, a US-based Atlantic Command would be outside the range of Russian conventional long-range strikes during a crisis.

Forward Logistics Command

The proposed logistics command would address NATO's challenge in moving and sustaining military forces across Europe, for exercises and training in peacetime and responding to Russian aggression or other contingencies during a crisis.

In recent years, NATO's difficulty in moving forces over strategic distances and sustaining them has become apparent. NATO member forces have been slowed by obstacles ranging from border bureaucracy and differing railway track gauges to weak bridges and narrow roads.

NATO's Eastern European operations and exercises also rely on massive amounts of supplies including fuel, munitions, spare parts and batteries. Stockpiles and infrastructure supporting these requirements in Eastern Europe have been lacking, although some measures have been taken to address this by the governments in Poland and the Baltic States, and as part of the United States' European Deterrence Initiative.

> Infrastructure imbalances have caused NATO operational troubles

The new logistics command would help address these shortfalls through coordination and planning across NATO members and commands. A formal decision is awaited, but Germany is an ideal candidate to host the new command. In the new European security environment, Germany is no longer a front-line state, as in the Cold War, but it is still relatively close to Eastern Europe and potential future crisis regions.

Germany has also indicated a willingness to take on this burden, as its role in European security continues to evolve quietly.

Cyber Operations Centre

Recent Russian military operations have included cyber elements in order to disrupt important military and societal functions, as well as to sow confusion and hesitation among the political leadership (see INTERNATIONAL: Moscow uses hacks to divide and confuse - June 28, 2017). In addition, the cyber domain forms an important part of Russian hybrid efforts aimed at both NATO and non-NATO members.

To date, NATO as an alliance has focused on providing cyber defence for its own network, while most offensive cyber capabilities have been developed and operated by individual member states. In particular, these are the United States, the United Kingdom, Germany and France.

NATO's envisioned Cyber Operations Centre is unlikely to develop its own cyber capabilities. Yet it would instead serve in a coordination role among the many national cyber tools and operations provided by the NATO member states.

In addition, the Cyber Operations Centre would help to integrate operations in the cyber domain along with those that would occur in the air, on land and in the maritime domain in response to a crisis with Russia or other competitors that are active in the cyber domain, such as China.

Iran is set to become a formidable cyber actor

Thursday, December 28, 2017

Iran's cyber capabilities have been steadily rising


Technicians monitor data flow in the control room of an internet service provider in Tehran February 15, 2011 (Reuters/Caren Firouz)

Tehran has invested in its technology sector in recent years to become one of the world's most cyber-capable nations. Though perhaps not on the same level as China and Russia, it is not far behind. Iranian hackers have carried out successful attacks in a number of countries, including Saudi Arabia and the United States.

What next

Iran is using increasingly sophisticated cyber capabilities to advance critical domestic- and foreign-policy goals. The government is committing substantial resources and learning the lessons of its own cyber vulnerabilities. That combination positions Iran to become an even more formidable cyber actor in the coming years.

Subsidiary Impacts

- Saudi Arabia is Iran's primary target for cyber operations, followed by Saudi supporters such as the United Arab Emirates and Bahrain.
- Iran will augment its own cyber warfare capabilities through proxies such as the 'Syrian Electronic Army'.
- US reversals over the nuclear deal may lead Iran to unleash a new wave of cyberattacks against US interests.

Analysis

Iran's cyber operations have been shaped by two separate but equally important domestic events.

The first was the extensive use of social media by opponents to organise protests in what became known as the 2009 Green Revolution. This was the most dramatic challenge to the ruling establishment since its ascent to power in 1979, and underscored that new technologies posed potential political threats. In the wake of protracted unrest, the government began extensive monitoring of mobile communications devices, social media and the internet, while blocking access to some websites.

The second salient event was the effectiveness of the Stuxnet operation, a joint US-Israel cyberattack to undermine Iran's nuclear programme discovered in 2010. This was malware placed in the main computers at the uranium enrichment facility at Natanz. The virus caused the IR-1 uranium enrichment centrifuges to spin wildly out of control. Nearly 1,000 centrifuges were destroyed, resulting in significant delays for the nuclear programme. Adding to the embarrassment, for months Iranian officials and scientists did not know what had caused such widespread disruption.

Investing in cyber capabilities

Those developments have prompted Iran to invest heavily in improving its own cyber capabilities since 2011. The elite Islamic Revolutionary Guard Corps (IRGC) claims to have added 120,000 cyber experts over the past five years. The government has also spent 1 billion dollars on increasing its cyber infrastructure and expertise. At least some of the training is coming from the growing number of skilled independent hackers working in concert with the IRGC.

The importance of expanded cyber capabilities to Iran was also reflected in the 2012 establishment of a Supreme Council of Cyberspace, which sets policies and priorities passed to the armed forces and IRGC. One of the council's first acts was to require identification and full names of anyone using internet cafes in Tehran.

The payoff

These investments are paying dividends. Iran has demonstrated major advances in cyber warfare compared with a decade ago. Its early cyber capabilities in the 2000s were limited mostly to unsophisticated distributed denial of service attacks. They are still used today against Israeli infrastructure targets such as water treatment and power plants, but they are not the most destructive of Iran's overall cyberattack capabilities.

Following the traumatic events of 2009-10, Iran adopted a more aggressive stance, starting with support to espionage operations. The vulnerability of military and financial databases such as the Saudi banking system provided a tempting and lucrative target set for Iranian hackers. Senior government officials in Bahrain, host to the US Fifth Fleet, have also complained privately that their defence ministry is subject to daily cyberattacks.

> Iran hackers specifically target aviation and energy firms

Of particular interest to Iran has been any information it may acquire on Western aviation technologies, which it has not been able to access because of years of international sanctions. US firm Fireye released a report in September 2017, in which it identifies a group named Advanced Persistent Threat (APT) 33 as Iranian. APT 33 has specifically targeted for espionage firms in the aviation and energy sectors in the United States, Saudi Arabia and South Korea (see INTERNATIONAL: State cyber threats will multiply - December 9, 2016).

Iran's most destructive cyberattack was the 2012 attack against Saudi Aramco, the world's largest oil company. The virus, Shamoon, crippled Aramco's business operations for weeks but did not disrupt production activities. Nonetheless, estimates suggest that up to 30,000 computers were rendered inoperable. The attack against Aramco coincided with a similar cyber strike against Qatar's natural gas producer RasGas.

Since that attack, US cybersecurity experts estimate that Iran's cyber capabilities have improved. The vice president of US firm Crowdstrike, Adam Meyer, assessed that Shamoon was a narrow and unsustainable campaign, but that since then Iran had been able to mount persistent attacks. He specifically said Iranian cyber operations since 2016 have sought to destabilise Saudi Arabia.

Iran has also been carrying out cyberattacks against major US banks, including the Bank of America, Wells Fargo and Capital One. The US Justice Department unsealed an indictment against seven Iranian nationals in conjunction with these attacks in 2016. One of the Iranians was also charged with plotting to disrupt the controls of the Bowman Avenue Dam in upstate New York. In 2014, casino magnate Sheldon Adelson's Las Vegas Sands Corporation was singled out for attack. Adelson is a prominent supporter of Jewish causes.

Attractive tools

In the volatile Middle East, cyberweapons are attractive precisely because their effects -- so far -- fall below the threshold of war. They are not seen by targeted nations as justifying the resort to force -- unless a cyberattack produces a similar level of physical destruction and loss of life as a conventional attack (see INTERNATIONAL: Cyber security faces concept challenges - December 19, 2014). Partly this is because it is difficult to attribute cyberattacks conclusively (see INTERNATIONAL: Impunity will incentivise cyberattacks - December 16, 2016).

> Cyber operations fall below the threshold of war

This provides a strong incentive for Iran to continue carrying out cyberattacks, since the chances of it being thrust into combat operations as a result are low.

Iran has demonstrated an impressive 'stand-alone' cyber capability. What comes next will likely be a closer integration of cyber capabilities into Iran's military strategy and doctrine. This will not happen overnight -- the United States and Russia have been pursuing a similar course for years -- and the ultimate extent to which Iran integrates cyber into military operational planning will be shaped by Tehran's regional threat perceptions and military requirements.

US security software protectionism will grow

Tuesday, October 3, 2017

Commercial incentives clash with national security concerns over Russian access to sensitive US cybersecurity software

Reuters reported yesterday that US software company Hewlett Packard Enterprise granted Russian regulators access last year to the source code for ArcSight cybersecurity software as part of the standard licensing process to sell to Russian public sector entities. The US Department of Defense uses the ArcSight software to detect and track unauthorised intrusions into US military networks. ArcSight is reportedly deployed on the department's Secret Internet Protocol Router Network (SIPRNet), which is used to transmit classified information. Hewlett Packard Enterprise reportedly did not inform the Pentagon of the source code inspection, which a Russian private contractor conducted on behalf of Russia's Federal Service for Technical and Export Control (FSTEC).

Our judgement

The US government, similar to many countries, is likely to impose more stringent controls on cybersecurity software procurement on national security grounds, balkanising global markets for such services. US software companies are likely to face increased restrictions on to whom they may sell if they wish to contract with the federal government, particularly as policymaker awareness of cybersecurity issues grows in light of the investigation into Russian interference in the 2016 US elections.

See RUSSIA: Internet will be subject to multiple controls - November 30, 2016

China's quantum leap will transform cybersecurity

Friday, September 8, 2017

China is at the forefront of global advances in quantum cryptography and communications


World's first quantum satellite launch in Jiuquan, Gansu Province, China, August 2016 (Reuters)

China's recent success with an experimental quantum communication satellite and other rapid advances in quantum cryptography are major steps towards its plans to construct national and global quantum networks that could, in theory, be close to unhackable.

What next

More quantum satellites will be launched and linked to the country's expanding fibre-optic quantum communications networks. China may become the first country to adopt quantum encryption on a large scale in government, military, and eventually even commercial use. However, the absolute security that the government seeks to achieve through these new networks may be elusive in practice.

Subsidiary Impacts

- Even if absolute security is impossible, quantum communications may still confer an edge.
- China could become less vulnerable to foreign nations' signals intelligence and cyber espionage capabilities.
- China's leadership in operationalising quantum cryptography is likely to create commercial opportunities -- for Chinese firms.
- In the more distant future (perhaps by 2030), China could take the lead in constructing a 'quantum internet'.

Analysis

The development of quantum cryptography, computing and sensing has been called 'the second quantum revolution'.

These disruptive technologies make use of 'quantum entanglement' and the 'no-cloning theorem'. Quantum entanglement is when the states of a pair or group of particles are strongly correlated so that their characteristics affect each other even if they are physically separated. The no-cloning theorem states that an unknown quantum state cannot be replicated.

Harnessing these properties for practical application enables unique technologies, of which quantum cryptography, and its use in quantum communications networks, is the most mature, having already entered actual use.

However, while the science is largely there and edging out of the labs and into engineering, putting it together in useful systems is at early stages, and commercialisation is likely at least 15 years off.

Quantum cryptography

The inherent qualities of quantum states make quantum cryptography almost uncrackable, at least in theory.

The most prevalent form is known as quantum key distribution (QKD), through which cryptographic keys are exchanged in quantum states through entanglement. The quantum information transmitted this way cannot be copied, and any attempted interference or eavesdropping can be detected.

This offers a secure mechanism for key exchange that can be used to encrypt communications using the conventional encryption techniques already in use.

QKD theoretically ensures perfect security, including against the future use of quantum computers, which will have the power to break most of the established forms of cryptography.

However, the promise of perfect security may not be matched in practice.

Still hackable

The substitution of conventional encryption by QKD does not eliminate vulnerabilities and weak links elsewhere in the system.

QKD has been difficult to implement beyond the laboratory and shortcomings in equipment or engineering could enable a hacker to exploit this notionally unhackable system.

There have even been several demonstrations of techniques to 'hack' or otherwise interfere with commercial quantum cryptographic systems, such as 'side channel attacks' and means of interception that remain below the expected error threshold or surreptitiously replicate data.

So far, detection of these potential loopholes has enabled measures to mitigate those vulnerabilities and better verify the security of quantum systems.

Chinese breakthroughs

Although the security of China's quantum networks is thus unlikely to be absolute, Chinese scientists have pursued new techniques that could enhance their reliability and overcome obstacles to practical use.

Leading quantum physicist Pan Jianwei and his colleagues last year reported advances in 'measurement-device-independent QKD', which uses decoy light pulses to detect attempted eavesdropping.

Two types of network

There are currently two main forms of quantum communications network. One uses QKD across nodes connected by optical fibres. The other is 'free space' quantum communications across open spaces.

Free space quantum communications, often between a ground station and satellite, enables communications at a greater distance and scale than optical fibres, but introduces potential interference from light, since quantum information is transmitted using photons.

China's quantum cryptography plans

China's government has placed quantum information science at the centre of its national security strategy, including it in the 13th Five-Year Plan's Science and Technology Innovation Plan and the new National Key Research and Development Plan. President Xi Jinping himself emphasised the strategic importance of quantum technologies to national security, particularly cybersecurity, when he visited Pan Jianwei's laboratory last year.

Quantum communications research gained importance after the Snowden leaks

The quantum communications research agenda gained importance after leaks by Edward Snowden revealed the extent of China's vulnerability to US signals intelligence and cyberespionage. The Snowden leaks were so fundamental to Chinese motivations that Snowden has been described in official media as one of two individuals with a leading role in China's advances in the domain (the other being Pan).

China's new quantum networks are already entering active use for sensitive defence, government and commercial communications at the metropolitan and regional level.

A quantum network that will stretch approximately 2,000 kilometres between Shanghai and Beijing, passing through Jinan, Hefei (where Pan is based) and other cities along the way, is reportedly on track to become fully operational imminently.

China's latest successes

China plans to use free space quantum communications to enable secure quantum networks of unparalleled scope and scale.

> Satellites allow quantum communications over much greater distances

In August 2016, China launched the world's first quantum satellite (see CHINA: West feels the force of China's space programme - December 21, 2015). The satellite, named Micius, established a QKD network through the transmission of quantum information between itself and multiple ground stations. This enables quantum communications at a greater distance.

Micius is a component of the Quantum Experiments at Space Scale (QUESS) project, initiated in 2011, which has involved collaboration between a team led by Pan Jianwei from the University of Science and Technology of China, the Chinese Academy of Sciences, and the Austrian Academy of Sciences. Use of quantum satellites was once restricted to night time due to interference from sunlight, but Pan's team has since resolved the 'nocturnal curse'.

Chinese scientists have reported successes in milestones for quantum information science through a series of experiments performed through Micius under the QUESS programme. They achieved ground-to-satellite quantum teleportation at a distance of 1,400 kilometres -- a critical step towards a global 'quantum internet'.

Micius was also used for the first ever space-to-ground QKD, in which quantum keys were sent from the satellite to ground stations at distances ranging from 645 kilometres to 1,200 kilometres, achieving a gain in efficiency of 20 orders of magnitude compared to optical fibre (see CHINA: Quantum satellite proves innovation capability - June 16, 2017).

China's advances in quantum cryptography could enhance its national information and communications security, if these new systems do prove to provide a distinct value added relative to classical alternatives, which will depend upon implementation and continued technological advances. Entanglement is a fragile phenomenon, and the difficulty of preserving it is a substantive challenge to the development of practical quantum information systems.

Oxford Analytica

Master the macroeconomic and geopolitical environment

We enable the world's leading organisations and governments to navigate complex global environments that impact strategy, policy, operations and investments.

What sets us apart

– In-house specialists harness our expert network to client advantage

– Robust methodology and founding principles keep us impartial

– Founded in 1975, our track record is unrivalled

Our key services

– The Oxford Analytica Daily Brief®

– Global Risk Monitor

– Advisory Services

– Training and workshops

– The Oxford Analytica Conference

COMPLIMENTARY ACCESS

Oxford Analytica is pleased to provide delegates of the Glasswall cyber dinner with one month's complimentary access to the **Oxford Analytica Daily Brief.**

Follow this link to sign up:
www.oxan.to/cyberdinner