Cyber Risk GmbH
Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341
Dammstrasse 16, 8810 Horgen, Switzerland
Tel: +41 79 505 89 60 Web: https://www.cyber-risk-gmbh.com

July 2021, top cyber risk and compliance related local news stories and world events

Dear readers,

I have just read for the second time some parts of the 7th edition of the US National Intelligence Council's Global Trends report. Published every four years since 1997, Global Trends assesses the key trends and uncertainties that will shape the strategic environment during the next *two decades*.

There is a very interesting part with title *"Disruptions in Employment"*. We read that the global employment landscape will continue to shift because of new technologies, notably automation, online collaboration tools, artificial intelligence (AI), and perhaps additive manufacturing.

Tasks that once seemed uniquely suited to human abilities, such as driving a car or diagnosing a disease, are already automated or potentially amenable to automation in the next decade. Studies have estimated that automation could eliminate 9 percent of existing jobs and radically change approximately one-third in the next 15 to 20 years.

Emerging technologies will also create jobs and will enable greater virtual labor mobility through Internet-based freelance platforms that match customers with self-employed service providers as well as speed-of-light commercial data and software transmission.

Demographics, specifically aging populations, will promote faster adoption of automation, even with increases in the retirement age. Most of today's largest economies will see their workforces shrink over the coming two decades as aging workers retire.

South Korea is projected to lose 23 percent of its working-age population (age 15-64), Japan 19 percent, southern Europe 17 percent, Germany 13 percent, and China 11 percent during this period, if the retirement age remains unchanged.

Automation—traditional industrial robots and AI-powered task automation—almost certainly will spread quickly as companies look for ways to replace and augment aging workforces in these economies.

Automation is likely to spread more slowly in other countries, with the key being whether it offers cost advantages, including over low-skilled labor.

The number of jobs created by new technologies is likely to surpass those destroyed during the next 20 years, judging from past episodes. One study by the World Economic Forum estimates that by 2025, automation will have created 97 million new jobs and displaced 85 million existing jobs.

Several factors, including skills, flexibility, demographic factors, underlying wages, the share of jobs susceptible to automation, and access to continuing education could influence how well individual countries are able to adapt to automation.

For example, countries with growing working-age cohorts are likely to experience more employment dislocations or downward pressure on wages than countries with older populations at comparable levels of automation.

Automation may affect a growing share of the workforce. During the past two decades, it has replaced mostly middle-skill job professions, such as machine operators, metal workers, and office clerks.

Automation may increasingly affect more high-income professions, such as doctors, lawyers, engineers, and university faculty.

Although new jobs will emerge, there is likely to be a skills mismatch between jobs lost and jobs created. This mismatch could lengthen the period of unemployment for many workers as they attempt to gain the

skills required for newly created jobs, and it could further skew the distribution of gains.

More youthful economies might be more agile if they are able to provide the education needed to properly train new entrants into the workforce.

In the part "Uncertain future of money" we read that digital currencies are likely to gain wider acceptance during the next two decades as the number of central bank digital currencies increase.

China's central bank launched its digital currency in 2020, and a consortium of central banks, working in conjunction with the Bank of International Settlements, is exploring foundational principles for sovereign digital currencies.

Read more at numbers 5 and 6 below.

How could the global economy evolve from here? What could "pandexit" look like?

Who asks questions like that? The new Annual Economic Report from the Bank for International Settlements (BIS).

How can we answer questions like that? We cannot, but we have to do our best, using financial stress testing. Of course, we will use adverse scenarios that are "severe yet plausible" (severe enough to be meaningful, yet plausible enough to be taken seriously).

We will follow Ovid's advice: *Perfer et obdura, dolor hic tibi proderit olim* - be patient and tough; someday this pain will be useful to you.

We read in the BIS Annual Economic Report that given the uncertainties involved, and before turning to policy, it is worth considering *three plausible scenarios*: the *central one* embodied in current consensus forecasts, *one* in which inflation proves stronger than expected and financial market conditions tighten, and *one* in which the global recovery falters and the economy fails to recover.

Of course, various combinations are also possible. The future will not be so tidy, and individual countries will experience different permutations. Even so, together the scenarios provide a useful range of plausible outcomes that helps clarify the challenges policymakers face.

Which are the three scenarios?

The *central scenario* sees a comparatively smooth recovery. The pandemic is steadily brought under control. Consumption sustains the expansion. Corporate sector losses remain limited, and sectoral reallocation proceeds smoothly.

In the main jurisdictions, inflation rises towards targets and any increase beyond them is temporary. Financial conditions do not tighten significantly. Even in this scenario, however, significant cross-country differences remain.

The world entered the crisis suddenly and as one; countries will "pandexit" at their own speed and in their own way. In particular, growth in many EMEs lags behind, even as some see more persistent inflation.

The *second scenario* is one where, on the back of stronger growth, inflation exceeds expectations and financial conditions tighten. Markets anticipate a quicker and possibly more intense monetary policy tightening.

This is consistent with a larger impact of fiscal policy on demand and a bigger reversal in saving rates than assumed in the central scenario, possibly supported by better news on the pandemic front.

How plausible is this scenario? To be sure, the longer-term forces holding inflation down are still with us, notably globalisation and technological advances: these have weakened the pricing power of both labour and firms.

Moreover, the responsiveness of inflation to pressures on productive capacity has been extremely low for well over a decade now. That said, non-linearities cannot be ruled out. And even if any increase in inflation ultimately proves temporary, financial market participants could overreact, anticipating more sustained inflation.

Either way, the tightening could be substantial, as participants could be caught wrong-footed and be forced to unwind their positions. The prolonged aggressive risk-taking that has prevailed in markets for so long increases the probability of such an outcome.

Recent localised stress, such as the Archegos failure and the losses it has inflicted on banks, could turn out to be the proverbial canary in the coalmine. A key question concerns the resilience of non-bank financial intermediation, especially in the context of hidden leverage and liquidity mismatches.

The *third scenario*, in which the recovery stalls, is more plausible if the

pandemic proves harder to control. Successive waves of more virulent Covid strains could be impervious to vaccines, leading to tighter containment measures.

Fiscal multipliers and the deployment of excess savings could fall short of expectations. In particular, the feared wave of firms' insolvencies could materialise – another big question mark clouding the outlook.

Estimates of likely credit losses embodied in the central scenario suggest that they would be manageable. Importantly, the debt in the most affected sectors accounts for a relatively small fraction of the total.

But this conclusion hinges on policy support being there for as long as necessary. In this alternative scenario, firms' losses could be larger, possibly on a par with those during the Great Financial Crisis (GFC).

In turn, banks could feel the strain. In fact, some of them have taken back part of the provisions made earlier in 2020, indicating that they could be caught by surprise.

Read more at Number 10 below.

From 10 to 21 May 2021, the Swiss National Cybersecurity Centre (NCSC) conducted a bug bounty pilot project in collaboration with Bug Bounty Switzerland GmbH, the Federal Department of Foreign Affairs (FDFA) and Parliamentary Services (PS).

The project was very successful and the lessons learned are to be incorporated into the implementation of further bug bounty programmes in the Federal Administration.

The purpose of bug bounty programmes is to identify, document and remedy any vulnerabilities in IT systems and applications in cooperation with ethical hackers. A total of 15 ethical hackers commissioned by the Confederation took part in this pilot project.

For the pilot project, ethical hackers scanned a total of six IT systems of the FDFA and Parliamentary Services for any security vulnerabilities. Overall, *ten* security vulnerabilities were reported to the NCSC. One of these turned out to be critical, seven were classified as medium and two as low.

All of the vulnerabilities were immediately eliminated by the competent providers. The ethical hackers then verified and confirmed the successful elimination of the vulnerabilities.

The pilot project demonstrated that vulnerabilities in IT systems and applications can be efficiently identified and remedied by means of bug bounty programmes.

The return on investment was found to be high. A bug bounty programme for the Federal Administration, operated by the NCSC, makes an important contribution to reducing the Confederation's cyber-risk exposure.

Based on the experience gained with the pilot project and the lessons learned by all those involved, the NCSC intends to continuously expand the bug bounty programme to as many Federal Administration systems as possible.

Consequently, the procurement process is to be launched as soon as possible. In the meantime, several other companies in Switzerland also offer bug bounty programmes in addition to Bug Bounty Switzerland GmbH.

In order to ensure neutrality in the procurement process, Florian Schütz, the Federal Cybersecurity Delegate, is thus stepping down from the Advisory Board of Bug Bounty Switzerland.

Have you read carefully the Situation Report of the Federal Intelligence Service, that was presented (in this newsletter too) last month? Today we publish a very important part of this report.

Increased vulnerability of the information infrastructure

The advance of digitalisation in the economy, in society and in public institutions is inexorable.

Digitalisation is underpinned and is being driven forward by technological development, which is constantly opening up new possible applications, and by the efficiency gains promised by digital solutions.

It is all-embracing and has become an unstoppable force, because without it linking up to the growing number of areas and processes that have already been digitalised is no longer possible.

Critical infrastructure operators across all sectors are under particular pressure to digitalise. As a result, analogue services are gradually being cut back.

The energy market is also investing in smart metering systems and power grids, and industrial control systems are being both operated and

maintained remotely.

In health care, the number of medical devices is increasing, as are technological advances including analytical devices which patients wear and operate themselves.

Coverage in Switzerland by the latest generation of mobile phone technology (5G) is being extended continuously, and trials are being conducted in a wide range of industries to assess the potential offered by artificial intelligence.

In order to avoid being left behind and missing opportunities and to cut costs, new technologies are being introduced rapidly.

Since spring 2020, this long-running trend toward digitalisation has been further accelerated by the measures taken to combat the pandemic.

The required restrictions on personal contact have led to increased demand for ways of working together virtually, such as video conferencing.

In order to minimise the risks to employees of becoming infected at the workplace or on the way there, a wide range of occupational groups have been provided with remote access to the information and systems relevant to their work, enabling them to work from home.

In many cases, technical, physical and organisational risks relating to information security were not fully taken into account – in the search for solutions, rapid availability was the primary deciding factor.

However, each new component in company networks and each additional system access option increases the number of vulnerabilities via which networks can be penetrated or systems disrupted.

Attacks on suppliers of critical infrastructure

Supply chain attacks continue to occur. Because interdependencies are growing and the security precautions of critical infrastructure operators are improving, companies which provide equipment and specialist services for critical infrastructure operators are becoming the attackers' preferred target.

There are numerous such companies in Switzerland, supplying operators in Switzerland and abroad. Their products are frequently used by multiple operators, and some suppliers have not yet invested enough to be able to guarantee their own security and that of their products.

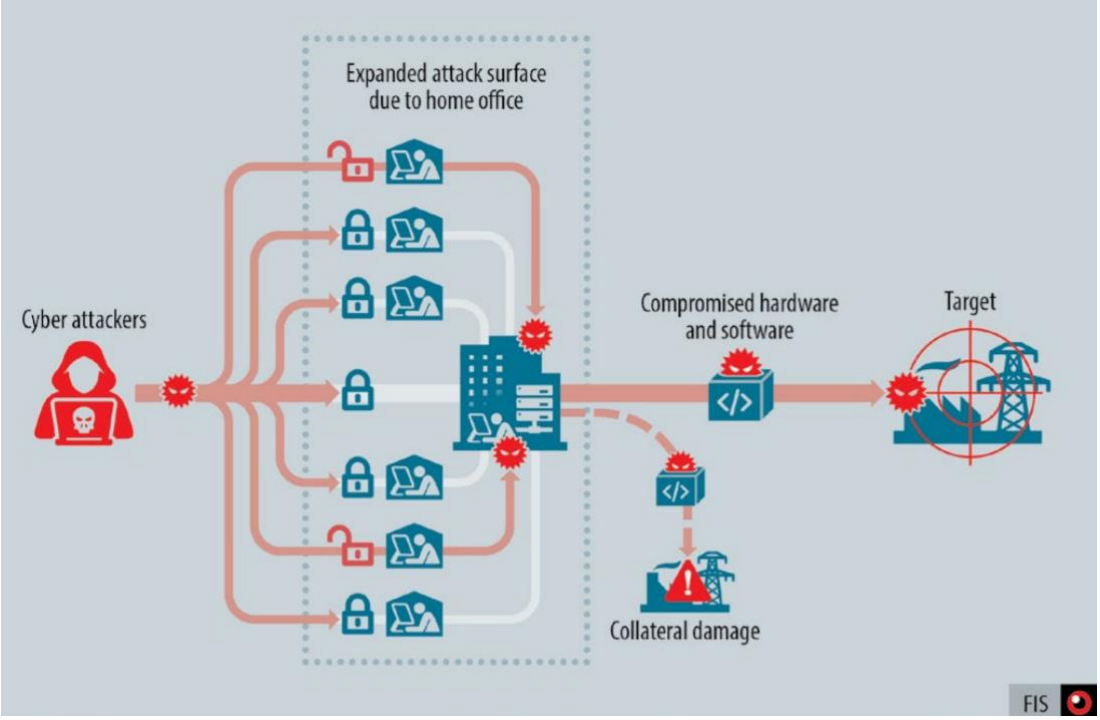
This makes them a rewarding target not only for criminal organisations but also for state-sponsored actors.

In accordance with the national strategy for the protection of Switzerland against cyber risks, Switzerland plans to establish a *National Test Institute for Cyber Security (NTC)*.

While the NTC will be able to check key items of equipment, this will be no substitute for the investment which is needed from Swiss suppliers in order to safeguard their own security and thus also that of the operators which are dependent on them.

In order to be able to take full advantage of digitalisation, Swiss companies must take greater account of the risks associated with it and of the measures for mitigating these risks.

Increasingly, this also applies to companies supplying critical infrastructure operators.



The increased usage of remote access, for example due to home office, expands the attack surface of networks.

Happy Birthday, Switzerland!

Switzerland celebrates its National Day (Schweizer Bundesfeiertag) on August 1. Celebrate together with your family and friends, enjoy the

barbecue together and the fireworks. It is good time to discover more about the history of the Swiss National Day.

Welcome to our monthly newsletter.

Best regards,

George Lekatis
General Manager, Cyber Risk GmbH
Dammstrasse 16, 8810 Horgen
Phone: +41 79 505 89 60
Email: george.lekatis@cyber-risk-gmbh.com
Web: www.cyber-risk-gmbh.com

Cyber Risk GmbH, Handelsregister des Kantons Zürich, Firmennummer: CHE-244.099.341

Number 1 (Page 13)

Cyber Security in a changing and complex world

Lindy Cameron, CEO, UK National Cyber Security Centre (NCSC), RUSI Annual Security Lecture

Number 2 (Page 25)

A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime

EU Serious and Organised Crime Threat Assessment (SOCTA)

Number 3 (Page 30)

EU Boost against cyberattacks: EU Agency for Cybersecurity welcomes proposal for the Joint Cyber Unit

The European Union Agency for Cybersecurity welcomes the European Commission proposal to launch the new Joint Cyber Unit which will act as a platform to ensure an EU coordinated response to large-scale cyber incidents and crises.

Number 4 (Page 32)

Authorities Seize DoubleVPN

Number 5 (Page 35)

Revisiting the 7th edition of the National Intelligence Council's Global Trends report.

Number 6 (Page 39)

National Intelligence Council's Global Trends report.

Emerging Dynamics

Societal:Disillusioned, informed, and divided

Number 7 (Page 45)

Unsecured servers and cloud services leave networks exposed to cyber attacks

Number 8 (Page 47)

A new notice in Search for rapidly evolving results

Danny Sullivan, Public Liaison for Search

Number 9 (Page 49)

NIST Method Uses Radio Signals to Image Hidden and Speeding Objects

Number 10 (Page 52)

BIS Annual Economic Report

Number 11 (Page 54)

Phishing most common Cyber Incident faced by SMEs

The European Union Agency for Cybersecurity identifies the cybersecurity challenges SMEs face today and issues recommendations.

Number 12 (Page 57)

Data of 700 million LinkedIn users reportedly advertised on dark web

National Cyber Security Centre

Number 13 (Page 59)

Thousands of fake online pharmacies shut down in INTERPOL operation

INTERPOL

Number 14 (Page 62)

Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments

National Security Agency | Cybersecurity & Infrastructure Security Agency | Federal Bureau of Investigation | National Cyber Security Centre a part of GCHQ

Number 1

Cyber Security in a changing and complex world

Lindy Cameron, CEO, UK National Cyber Security Centre (NCSC), RUSI Annual Security Lecture

It's great to be back here at RUSI (albeit virtually), at the world's oldest independent defence and security thinktank. It's a real privilege to be giving the second Annual Security Lecture.

And a particular privilege to follow the deeply impressive Dame Cressida Dick, who last year talked about the increasing influence and opportunity of data and technology in modern policing – at a time where a growing proportion of crime in the UK is either digitally enabled or committed entirely online.

We work in close partnership with law enforcement, so it won't surprise you that my lecture today will also look at cyber threats and opportunities. But I also look forward with hope to the day soon when it's unremarkable to have two senior women giving a lecture on national security. We're on our way but not there yet.

I'm also very proud to be here as the second head of the National Cyber Security Centre, which after only five years plays a key role in the UK's national security.

Its creation in 2016 showed real foresight and is widely recognised as an example others want to emulate – a partnership of government, law enforcement, intelligence and the private sector. And we have achieved a huge amount since then.

We have dealt with over 2,000 significant incidents.

We have protected the UK at scale through Active Cyber Defence – taking down more than 700,000 online scams in the last year alone, 80,000 of which were new tip offs from the British public through the hugely successful Suspicious Email Reporting Service.

We have raised resilience in all sectors of our critical national infrastructure, and built coalitions with businesses, charities and education to develop accessible and actionable cyber security tools and advice.

Over 55,000 teenagers have participated in the CyberFirst Girls competition and our cyber security courses.

And we have made the internet safer and easier to use for UK citizens through our Cyber Aware campaign, challenging password culture and victim blaming.

So I'm not sure if you planned it like this, but this feels like a really important moment to be talking about cyber security - and about cyber security as an international and not just a national issue, as an issue of mainstream national security policy.

As the Attorney General said in his landmark 2018 Chatham House speech on international law in this area, the influence of cyberspace on international relations is 'growing not shrinking.'

Of course the UK has seen cyber security as a mainstream national security issue for some time, key to our strategy, statecraft and the expression of our national values.

This was clear in the 2016 Cyber Security Strategy, which drove institutional change and investment. But the recent Integrated Review of Security, Defence, Development and Foreign Policy was even clearer on the importance of cyberspace in protecting our core interests of sovereignty, security and prosperity.

It outlined a vision of the UK, more robustly resilient to the threats of a competitive world, but also better able to take advantage of its opportunities, and working with allies to shape that world for the benefit of all.

Don't just search for the 'cyber' section of the integrated review – stand back and understand how fundamental the ability to operate in cyberspace is to the whole vision, underpinned by investment in the UK as a global science and technology and responsible cyber power.

You will have heard key interventions by the Foreign Secretary and Home Secretary last month at the NCSC's flagship CYBERUK conference – livestreamed on YouTube – and still available – and seen many interventions just in the last week from the Foreign Secretary, Defence Secretary and alumni of the national security community.

What is changing is that the international consensus on this is building. You can see that today as NATO leaders meet to agree how to adapt further to cyber challenges and how to strengthen the resilience of the alliance, in

the language used by leaders at the G7 summit at Carbis Bay in Cornwall, and in the prospect of a G7 Future Tech Forum.

The G7 and like minded partners are both calling out cyber threats and promising to work together on cyber opportunities like future technical standards that are in line with our core values.

This is particularly true of the incoming Biden administration, one of whose very first national security challenges was the response to the SolarWinds intrusion, and who in recent days have, in the words of Deputy National Security Adviser Anne Neuberger 'stepped up' their response to ransomware in the face of live examples of the cyber threat to critical national infrastructure like the Colonial Pipeline, issuing a wide ranging cyber Executive Order.

We have seen the nomination of influential experts like Chris Inglis, author of the Cyberspace Solarium Commission report, and Jen Easterley, to key positions in the new administration. And a recognition that cyber security requires the same kind of joined up, nationally coordinated whole of government response as counter terrorism – although the threats are very different.

So there is a moment now, to take our alliances in this space to a different level. And we in the UK are well positioned to play a key leading role in this. One of our strengths, in my view, is that we consistently treat cyber security not just as a national security issue but as a mainstream public policy issue, where – for example – success in the education sector is as important as more traditional national security concerns.

The UK's Integrated Review is really clear on this: it talks about "pursuing a whole of nation effort, bringing together industry and academia in partnership" and "engaging citizens, who have a central role to plan in our national security".

I see our other key strength as the centrality of resilience in our strategy – recognising that we need to 'make the UK the safest place to live and work online' for everyone – citizens and businesses as much as government.

That is not to say we are perfect – as I have said before, there is no room for complacency, and we have much more to do. But we know our approach works, and we should bring others with us on this journey.

So it is very prescient and rather timely of you here at RUSI to choose this issue for your second annual Security Lecture. And thank you for choosing me.

Those of you who know me and my background – and of course I'm not unfamiliar with RUSI and its members – will know that my entire career has been about a 'whole of nation' approach, whether at home or internationally.

So I hope that, despite being an illustrious security and defence thinktank, you are not expecting me to see cyberspace purely as a war zone, or my lecture to be filled with gory battlefield imagery.

Others can do that far better than me. My career in national security has always been about the messy reality of people's everyday lives and the transformative potential of economic growth, even in conflict.

And that's why, as you can imagine, when I look at cyberspace, I don't see the threat as being confined to state actors. That is not in any way to underestimate the scale or seriousness of state activity or data theft.

It consumes a very significant part of my team's most sophisticated capability. State sponsored cyber activity represents one of the most malicious strategic threats to the UK's national interests.

It is hugely important. Tracking and defending the UK from our most sophisticated adversaries represents much of our core business, usually working to support victims behind the scenes.

But it is not the only threat. And if we treated it as such, we would misrepresent the totality of the challenge and run the risk of an inappropriate response.

Firstly because we all know that looking at a conflict solely through the lens of the protagonists would be to miss the inevitable opportunistic criminals exploiting the black market. And secondly because cyberspace is – primarily - a peaceful domain, of prosperity and opportunity. And that should tell us something profound about what we need to protect: the aggregation of economic harm to individuals and organisations.

The UK digital sector employed 1.5m people and added £150bn to the UK economy in 2019. And that's true not only in the UK, but internationally.

And of course – as this audience will be well aware - state actors are a reality in cyberspace. Four nation states – China, Russia, North Korea and Iran, have been a constant presence in recent years. And as I've said before, we face a determined, aggressive Russia, seeking traditional political advantage by new, high-tech means.

We live in a business and corporate environment where Chinese cyber attacks on our commercial interests are something our companies treat as business as usual.

And authoritarian regimes including North Korea and Iran use digital technology to sabotage and steal.

This is not a surprise, and it's not new. Of course, you as a think tank will know this. A recent NCSC assessment of the Threat to Think Tanks noted it is 'almost certain' that the primary cyber threat to UK think tanks is from nation state espionage groups and it is 'highly likely' that they will seek to gain strategic insights into government policy, trade agreements and commercially sensitive information. So it's not just governments that are at risk.

But it's no longer 'just' espionage and data theft that is a threat. Even where it is, the complexity of modern supply chains may mean that many others can be caught in the crossfire and suffer compromises to their systems, as we saw with the recent SolarWinds Orion compromise and subsequent targeting, attributed as being 'highly likely' the work of the Russian intelligence services.

So although the threat has grown, our investment in cyber security means we know more about these threats now than we did five years ago when the NCSC was set up. And our world leading systems for sharing information with trusted partners means we can use this to improve the resilience of businesses and civil society, not just government and critical national infrastructure. Our ability to do this is the envy of many.

We have also used this knowledge to contribute to a series of public attributions that have exposed state activity -including attributing Not Petya and the DNC hack to Russia; the APT10 intrusion set to China; Wannacry to the North Korean Lazarus Group and the Mabna Institute to Iranian actors.

Attribution is part of our approach to cyber deterrence, as previous Foreign Secretaries have laid out. We seek to discover who is behind activity; expose the detail of their action in a way which helps both public and private sector defend; prosecute where possible, and – when we choose to – respond.

Because although building cyber resilience is crucial, the government also needs the capability to take action directly to counter a range of threats – a 'whole of cyber' approach. And that's why one of the range of strategic outcomes supported by the new National Cyber Force's cyber operations is cyber security, working in close partnership with us at NCSC.

So what I find most worrying isn't the activity of state actors. Nor is it an improbable cyber armageddon – though if you want a good description of a sort of dystopian, Blade Runner style future, check the attention-grabbing opening pages of the Solarium report.

What I worry most about is the cumulative effect of a potential failure to manage cyber risk and the failure to take the threat of cyber criminality seriously.

For the vast majority of UK citizens and businesses, and indeed for the vast majority of critical national infrastructure providers and government service providers, the primary threat is not state actors but cyber criminals, and in particular the threat of ransomware.

This has become more evident than ever during covid – that we need to focus on victims not just threat, and that small harms can amount to a cumulative risk of national significance.

This is the most insidious cyber security risk – not the threat from, but threat to; and not the loss of data but the impact on operations, large and small, that stops people and business from being able to live their day to day lives.

The sheer volume makes it the most impactful threat we face. We have seen it affect the NHS with WannaCry, prevent students accessing classes in the last few weeks, and shut down local authorities at great cost to the public purse, meaning the public cannot access services, pay their bills or, in some cases, even buy a house.

Ransomware has historically been the preserve of high-end cyber crime groups with access to advanced technical skills and capabilities based in overseas jurisdictions who turn a blind eye or otherwise fail to act to pursue these groups.

But the ecosystem is evolving through what we call Ransomware as a Service, (RaaS) and the 'As a Service' business model where ransomware variants and commodity listings, such as lists of credentials, are available off the shelf for a one-off payment or a share of the profits.

We know that there are campaigns to recruit new affiliates. As a result, users buy from developers without the costs and risks of developing it themselves, and that enables actors less experienced in ransomware to acquire tools to conduct their own attacks.

As the business model has become more and more successful, with these groups securing significant ransom payments from large and profitable

businesses who cannot afford to lose their data to encryption or to suffer the down time while their services are offline, the market for ransomware has become increasingly 'professional'.

If your files are encrypted by ransomware you may be offered the services of a 24/7 help centre to quickly pay the ransom and get yourself back online. The ransom note accompanying the attack gives you the contact details to use to negotiate with the attackers and unlock your files. Everything is geared to make it as easy as possible to simply pay the ransom and move on.

High end crime groups spend time conducting in depth reconnaissance on their targeted victims. They will identify your cyber security weaknesses that they can exploit. They will use spoofing and spearphishing to masquerade as internal employees to get access to all of the networks they need.

They will look for the business-critical files to encrypt and hold hostage. They may identify embarrassing or business sensitive material that they can threaten to leak or sell to others. And they may even research your cyber insurance policy to see if you are covered to pay ransoms.

This process can be painstaking and lengthy, but it means that, when they are ready to deploy, the effect of ransomware on an unprepared business is brutal. Everything is taken out. Files are encrypted. Servers go down. Digital phonelines no longer function. Everything comes to a halt and your business stops in its tracks.

Some of the most powerful testimonies I've heard since starting this job have been from chief executives faced with a ransomware attack they were under-prepared for.

We support victims of ransomware every day, but turning up to a ransomware incident as the NCSC feels like the fire service turning up to a house that has already burned down. There might be some forensic evidence that the police might pursue.

Occasionally (but less so over time) there might be a flaw in the malware or its deployment that we can make the most of. Even more rarely, we just might be able to get a decryption key. But these groups know what they're doing, and that hardly ever happens. More often than not, it's a case of rebuilding from scratch and restoring the data – assuming you have – and please read the advice – an offline backup that can be used for this.

But it doesn't stop there. Over the last year or so these cyber crime groups have evolved their techniques to include data extortion. Even if you have

offline backups and can get back on your feet without paying a ransom, the group will threaten to leak the data they have stolen.

This can make all your business information, personal sensitive data, otherwise embarrassing content, available online for all to see. So, this is now the double whammy of ransomware; even if you have good data storage in place they can still try and hold you to ransom.

Many victim organisations in this situation feel they have no choice but to pay. It's the same emotional blackmail technique that con-artists play on vulnerable elderly people they are trying to extract bank details from.

I have huge sympathy for how that must feel. But paying a ransom in no way guarantees the return of data (which unlike a human kidnap victim, can be copied). And it funds a criminal enterprise which will be encouraged to try the same thing on others.

This isn't a counsel of despair. In some respects, our response to ransomware is straightforward: we need to continue to build the UK's cyber resilience so that attacks cannot reach their targets in the first place. We have great advice on how to do this with our 10 Steps to Cyber Security and we've made huge strides across a range of sectors.

And it's about preparing, planning and exercising, all the way up to Board level, working on the assumption that a cyber criminal will be as interested in your weaknesses as a burglar is in your open window.

Reporting really matters – even if you are a victim and it's too late to limit the damage to your business, it helps us help others. All this not only helps make businesses resilient to ransomware, but to the full range of cyber threats they face, and deters adversaries by increasing the cost of an attack.

But in many other respects it requires a whole of government response. This starts with the efforts to prevent the activities of the groups behind these damaging attacks. These criminals don't exist in a vacuum.

They are often enabled and facilitated by states acting with impunity. International and diplomatic efforts need to be coordinated to stop them. And it includes seeking the strongest criminal justice outcomes for those we apprehend. There are other players with a key role such as the cyber insurance industry which has a role to play in bearing down on the payment of ransoms and cryptocurrency entities who facilitate suspicious transactions.

There will also be a role for cyber operations, taking direct action alongside law enforcement; disrupting cyber crime marketplaces where criminals buy and sell credentials, and disrupting ransomware groups.

None of this is a substitute for effective cyber security, but it is an increasingly necessary part of the national toolkit and a whole of nation approach. And that national approach must be coordinated with others, as the Foreign Secretary outlined in his interview with the Telegraph last week, and indeed as the G7 communique lays out.

A coordinated response on ransomware, involving these key players, would have the added benefit of helping us meet broader national and strategic international objectives, making the UK a more resilient and prosperous place to live and do business online.

And it's vital we recognise this - because we are at inflection point in global technology. Jeremy Fleming, Director of GCHQ, described a 'moment of reckoning' recently, where without action the key technologies we rely on won't be shaped or controlled by the likeminded democracies.

We already know proliferation is a risk. We know there are companies that sell high end state-like capabilities that exploit computer networks and at the other end of the spectrum, you can buy an 8 radio SIMBox for $300 which allows you to send thousands of cyber crime SMS campaigns every hour. These things won't just matter to UK customers, they matter globally.

But we also know that in every era of the internet we have struggled to anticipate the magnitude or speed of change ahead of us. Back in the 1980s when I was loading computer games onto my ZX Spectrum+ using a cassette recorder I couldn't have imagined a mobile phone, let alone an Apple Watch.

So that's why the UK is leading the way in anticipating the potential scale of change in the future. And as I said, this needs to be a whole of nation approach. Let me give you three examples where government can play a role.

Firstly, the Internet of Things. On Consumer IoT devices, we have developed a cyber security standard now embedded in draft legislation that products sold in the UK will have to meet. That has become a European, and we hope, a global standard. We want to see the same radical change in assumptions about the security of internet connected devices as we've seen in car safety for baby seats over the last decades.

Secondly, the new Telecoms (Security) Bill will see a regulatory framework place security requirements on how telecoms operators build and run their

networks. No one has taken it to this level before - it will create the toughest telecoms security regime in the world.

It will provide new legal powers in two parts: a new security regime with a range of new security duties on operators and new monitoring and enforcement powers for Ofcom. And new national security powers, replacing the thus far voluntary arrangement between the government and operators, to remove and restrict use of goods, services, and equipment from vendors designated as high risk. Non-compliance could result in fines of up to 10% of turnover or a daily penalty of £100,000.

The National Security and Investment Act, the biggest shake-up of the UK's investment screening regime in 20 years, will modernise government's powers to investigate and intervene in potentially hostile foreign direct investment, while advancing the UK's world-leading reputation as an attractive place to invest.

Of the 17 sectors it covers, those most important for cyber security (and where we were instrumental in developing the definitions) are Artificial Intelligence, computing hardware, data infrastructure, communications, quantum technologies and crypt authentication.

That helps us protect our critical services from cyber-attacks and improve the underlying security of the Internet through technological improvement.

But government cannot do this alone. We will continue to take a whole-of-society approach to improving the cyber resilience of the UK: industry, academia, and civil society all have a role to play.

While government is uniquely able to disrupt and deter our adversaries, it is network defenders in industry, and the steps that all organisations and citizens are taking that are protecting the UK from attacks, day in, day out. The protection they provide is crucial to the digital transformation of the economy, and every organisation, large and small, has a role to play.

We have come a long way, but there is room for improvement, and for even deeper collaboration. I hope the review of the Computer Misuse Act announced by the Home Secretary will help with this.

Yet collaboration cannot end at our borders; UK cyber resilience is not just a UK challenge. This is a global challenge and we cannot do this alone. We must continue to deepen our partnerships with partners around the world to support of our mutual resilience, both in response to the immediate ransomware threat but also to the longer term benefit of all of our economies and societies.

It's fantastic to see the consensus building that cyber security is a leader-level national security issue, as we have done in the last few days at the G7 and Nato. There is probably a whole other speech to give on what more we can do to build on that consensus and momentum, which I don't have time to do full justice to today. But in summary, I think what we can do is to:

Firstly, agree what's acceptable. As the G7 communique flags we need to work together to further a common understanding of how international law applies to cyberspace. We need to do the work as a global community to clarify and develop rules that are right for the digital age and the Foreign Secretary has made clear the UK plans to lead on this.

I therefore welcome the UN Government Group of Experts on cyberspace reaching its first agreement since 2015, building on the global appetite for clear appetite for progress captured in the consensus report by the Open Ended Working Group earlier this year.

Secondly, we need to set standards more effectively. Whatever model of standards body we are talking about – government led, industry only or genuinely multistakeholder - they are critical to the future of technology, including interoperability and security.

The UK prefers multi-stakeholder bodies because that brings balance. This is not about government control – this is about upping our engagement in a way that will benefit our prosperity and security and uphold our values.

And thirdly we need to build alliances. We already have fantastic partnerships with our 5 eyes allies and through NATO. Based on trust, collective action and a shared vision for the future.

But for a whole of nation partnership approach and to deal with the challenges of cyber security in a rapidly changing world, we must also deepen our partnerships with like-minded European countries, partners in Asia and beyond.

So in conclusion:

This really does feel like the moment when the world starts to take cyber security seriously, as a national security issue and a public policy issue.

As I have been clear, I see cyberspace primarily as a domain of civic and commercial interaction that enables economic growth and wider societal benefits, and that must remain free, open, peaceful and secure.
It is a real moment of opportunity, despite the current focus on threats.

And for the UK, it is also a moment of leadership. We are ahead of the game – we have invested in cyber security and set ourselves up for success. We have a whole of nation strategy with resilience at its core and we must deliver on that.

And with our new cyber strategy this year, we will have a chance to lay out how we see the future in more detail. I look forward to NCSC playing our part in that future.

Yoy may visit: https://www.ncsc.gov.uk/speech/rusi-lecture

Number 2

A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime

EU Serious and Organised Crime Threat Assessment (SOCTA)

The EU Serious and Organised Crime Threat Assessment (SOCTA) is the product of systematic and comprehensive analysis of law enforcement information on criminal activities and networks affecting the EU.

The SOCTA is designed to assist decision-makers in the prioritisation of serious and organised crime threats.

It has been produced by Europol, drawing on extensive contributions from the organisation's databases and external partners. Europol would like to express its gratitude to Member States, non-EU countries, EU agencies and institutions and international organisations for their valuable contributions and input.

The EU SOCTA 2021 is the outcome of a detailed analysis of the threat of serious and organised crime facing the EU, providing information for practitioners, decision-makers and the wider public. As a threat assessment, the SOCTA is a forward-looking document that assesses shifts in the serious and organised crime landscape.

The SOCTA 2021 sets out current and anticipated developments across the spectrum of serious and organised crime, identifies the key criminal groups and individuals involved in criminal activities across the EU and describes the factors in the wider environment that shape serious and organised crime in the EU.

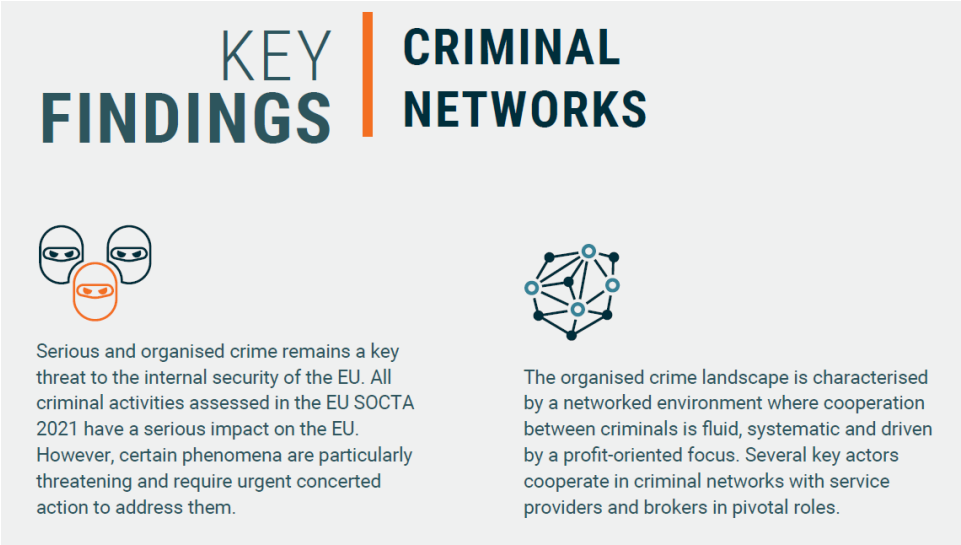
The SOCTA 2021 provides an overview of the current state of knowledge on criminal networks and their operations based on data provided to Europol by Member States and partners and data collected specifically for the SOCTA 2021.

In trying to overcome the established, and limiting, conceptualisation of organised crime groups, this assessment focuses on the roles of criminals within criminal processes and outlines how a better understanding of those roles allows for a more targeted operational approach in the fight against serious and organised crime.

- Close to 40% of the criminal networks active in the EU are involved in the trade in illegal drugs.

- Around 60 % of the criminal networks active in the EU use violence as part of their criminal businesses.

- The use of corruption and the abuse of legal business structures are key features of serious and organised crime in Europe. Two thirds of criminals use corruption on a regular basis. More than 80 % of the criminal networks use legal business structures



Similar to a business environment, the core of a criminal network is composed of managerial layers and field operators. This core is surrounded by a range of actors linked to the crime infrastructure providing support services, such as brokers, document fraudsters, technical experts, legal and financial advisors, money launderers and other service providers.

A key characteristic of criminal networks, once more confirmed by the pandemic, is their agility in adapting to and capitalising on changes in the environment in which they operate. Obstacles become criminal opportunities and may be as simple as adapting the narrative of a known modus operandi.

The use of violence by criminals involved in serious and organised crime in the EU appears to have been increasing in terms of the frequency of use and its severity. Criminals use violence indiscriminately and target victims without regard for their involvement or standing, often accepting harm to innocent bystanders. The threat from violent incidents has been augmented by the frequent use of firearms or explosives in public.

Corruption is a feature of most, if not all, criminal activities in the EU. Corruption takes place at all levels of society and can range from petty bribery to complex multi-million-euro corruption schemes. Corruption erodes the rule of law, weakens institutions of states and hinders economic development. Corruption is a key threat to be addressed in the fight against serious and organised crime. Almost 60 % of the criminal groups reported for the SOCTA 2021 engage in corruption[2].

The scale and complexity of money laundering activities in the EU have previously been underestimated. Serious and organised crime in the EU fundamentally relies on the ability to launder vast amounts of criminal profits. For this purpose, professional money launderers have established a parallel underground financial system to process transactions and payments isolated from any oversight mechanisms governing the legal financial system. This parallel system ensures that the criminal proceeds cannot be traced as part of a sophisticated criminal economy.

Legal business structures such as companies or other entities are used to facilitate virtually all types of criminal activity with an impact on the EU. Criminals directly control or infiltrate legal business structures in order to facilitate their criminal activities. All types of legal businesses are potentially vulnerable to exploitation by serious and organised crime. More than 80 % of the criminal networks active in the EU use legal business structures for their criminal activities. About half of all criminal networks set up their own legal business structures or infiltrate businesses at a high level.

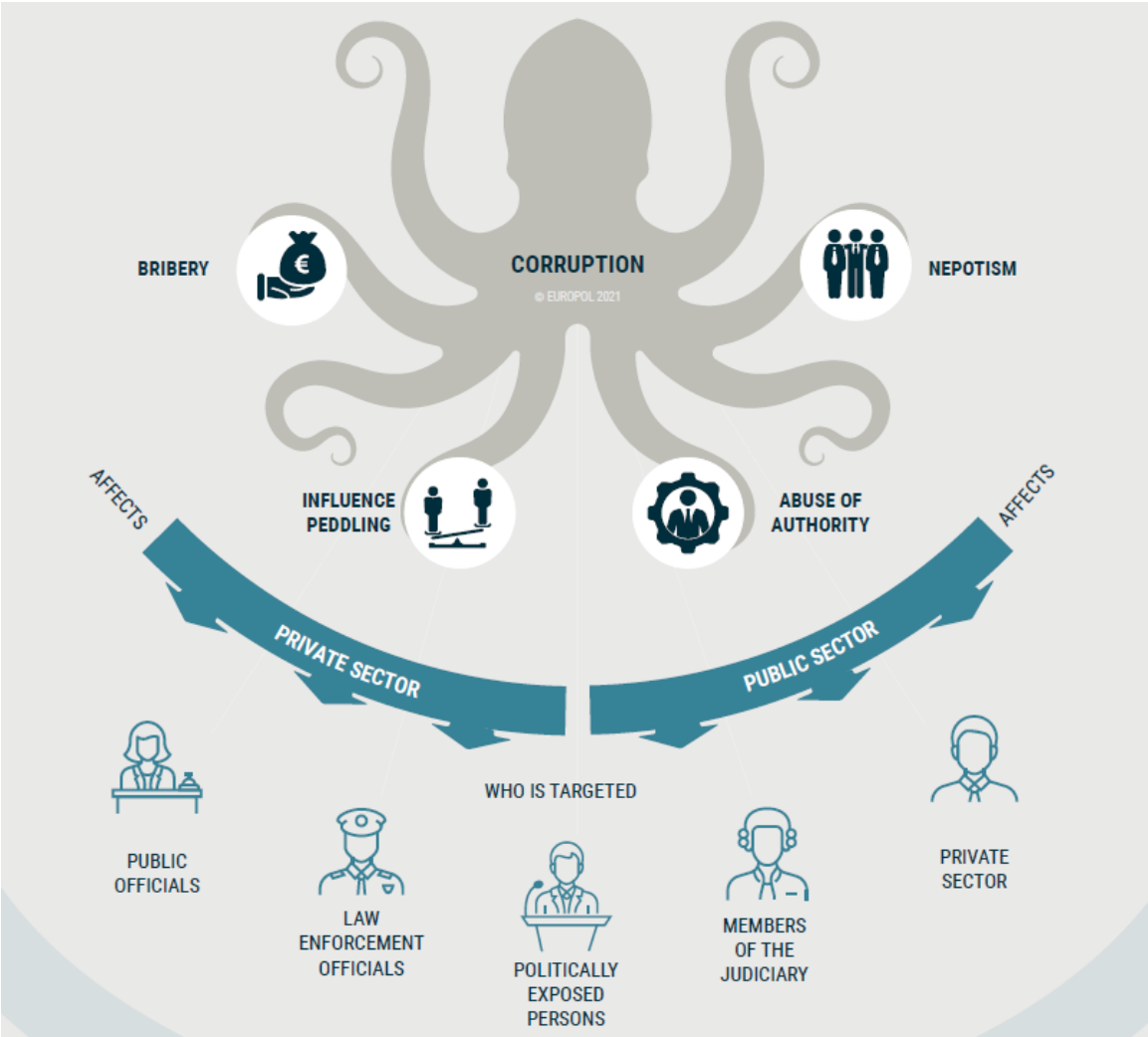
The use of technology is a key feature of serious and organised crime in 2021. Criminals exploit encrypted communications to network among each other, use social media and instant messaging services to reach a larger audience to advertise illegal goods or to spread disinformation. The online environment and online trade provide criminals access to expertise and sophisticated tools enabling criminal activities.

A potential deep economic recession following the COVID-19 pandemic will fundamentally shape serious and organised crime in the EU for the near future. Previous periods of economic stress can provide some degree of insight into how these developments might affect crime in the EU and what responses need to be formulated to counter existing and emerging threats to the EU's internal security during this time.

The threat from **cyber-dependent crime** has been increasing over the last years, not only in terms of the number of attacks reported but also in terms of the sophistication of attacks. Cyber-dependent crime is likely significantly underreported. The rapidly progressing digitalisation of society and the economy constantly creates new opportunities for criminals involved in cyber-dependent crime. Fraud schemes take advantage of the digital era. Online fraud schemes target private individuals, businesses and public sector organisations.

The COVID-19 pandemic has had a significant impact on the serious and organised crime landscape in the EU. Criminals were quick to adapt illegal products, modi operandi and narratives in order to exploit the fear and anxieties of Europeans and to capitalise on the scarcity of some vital goods during the pandemic. While some criminal activities will or have returned to their pre-pandemic state, others will be fundamentally changed by the COVID-19 pandemic.

Serious and organised crime deeply affects all layers of society; in addition to the direct impact on the daily lives of EU citizens, it also undermines the economy, state institutions and the rule of law.



To read more: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

Number 3

EU Boost against cyberattacks: EU Agency for Cybersecurity welcomes proposal for the Joint Cyber Unit

The European Union Agency for Cybersecurity welcomes the European Commission proposal to launch the new Joint Cyber Unit which will act as a platform to ensure an EU coordinated response to large-scale cyber incidents and crises.

The concept of the Joint Cyber Unit (JCU), suggested two years ago by European Commission President von der Leyen, is an important step towards completing the European cybersecurity crisis management framework.

The EU Agency for Cybersecurity (ENISA) welcomes the proposal for the Commission Recommendation to build a Joint Cyber Unit and the role it is foreseen to play.

The Cybersecurity Act mandates the Agency to cooperate at the operational level and establish synergies with Union institutions, bodies, offices and agencies. The JCU helps the Agency to achieve this in a structural manner.

The support the EU Agency for Cybersecurity would provide to building a Joint Cyber Unit comes as a reinforcement of the provisions set out in the Cybersecurity Act, which has widened the scope of the activities of the Agency. This new initiative is an important step on how the Agency can further contribute to achieve a higher common level of cybersecurity within the European Union.

Margrethe Vestager, Executive Vice-President for a Europe Fit for the Digital Age, said: "Cybersecurity is a cornerstone of a digital and connected Europe. And in today's society, responding to threats in a coordinated manner is paramount. The Joint Cyber Unit will contribute to that goal. Together we can really make a difference."

Margaritis Schinas, Vice-President for Promoting our European Way of Life, said: "The recent ransomware attacks should serve as a warning that we must protect ourselves against threats that could undermine our security and our European Way of Life. Today, we can no longer distinguish between online and offline threats. We need to pool all our resources to defeat cyber risks and enhance our operational capacity. Building a trusted and secure digital world, based on our values, requires commitment from all, including law enforcement."

Thierry Breton, Commissioner for the Internal Market, said: "Today we have put in place an ambitious building block in protecting ourselves from cyber threats that are evolving rapidly and are becoming more complex. We have set clear milestones and timelines that will allow us to concretely improve crisis management cooperation in the EU. The Joint4 Cyber Unit leverages the expertise that is scattered across Europe and will enable us to not only detect threats but also react faster."

Juhan Lepassaar, EU Agency for Cybersecurity Executive Director said: "The EU Agency for Cybersecurity is committed to support the Union and its Member States in the response to cyberattacks. The Joint Cyber Unit will build stronger relationships within the cybersecurity ecosystem and shape an effective framework for crisis management. Our future local office in Brussels will operate closely with the Unit to coordinate response, create situational awareness and ensure preparedness in times of crisis."

Number 4

Authorities Seize DoubleVPN

On 29th of June 2021, law enforcement took down DoubleVPN. Law enforcement gained access to the servers of DoubleVPN and seized personal information, logs and statistics kept by DoubleVPN about all of its customers. DoubleVPN's owners failed to provide the services they promised.

International law enforcement continues to work collectively against facilitators of cybercrime, wherever and however it is committed. The investigation regarding customer data of this network will continue.

These were the "services" offered previously:

Simple

The first (the only) server receives request from your computer and sends it on its behalf into the Internet.

- No logs or statistics kept!
- Maximum connection speed with good anonymity
- Access to our private anonymous dns server

Learn more

from 25$ per month

Order Simple

Double

The first server receives request from your computer and redirects it to the second server, which sends it on its behalf into the Internet.

- No logs or statistics kept!
- Best connection speed/anonymity combination
- Access to our private anonymous dns server

Learn more

from 36$ per month

Order Double

Triple

The first server receives request from your computer and redirects it to the second, the second redirects to the third, which sends it into the Internet.

- No logs or statistics kept!
- Maximum anonymity
- Access to our private anonymous dns server

Learn more

from 42$ per month

Order Triple

What are our advantages?

Maximum security
We protect you from traffic interception at home, at work or in public Wi-Fi. Neither ISP, nor criminals, nor public Wi-Fi owners will be able to learn your credit card number or social network message.

Anonymity guaranteed
We make your internet surfing anonymous by changing your external IP address. So it doesn't reveal your real location and keeps secret your internet surfing history.

We don't spy on our clients
We can speak responsibly that there is no logging client activity on our servers. That's why we are ready to provide you with direct access to any our server.

Bypass ISP site blocking
With our service you can access the content which is blocked by your government censorship, system administrator at work or ISP at home.

Unlimited traffic
We don't have traffic limitations and the server bandwidth is distributed among clients depending on their needs. You can watch or download video, music and other digital content.

Fabulous connection speed
A wide range of choice of servers in different countries with large bandwidth and real hardware guarantees fast and stable work.


No third parties
We have rather high prices because client payments for subscriptions is our only source of income. Ask yourself: where do free or cheap vpn services get money from to pay for their expenses?
Discounts and sales
We often run sales with discounts wich add to your discount program. So you can buy subscriptions about twice cheaper during some of our sales. Keep an eye on our service news.
Discount program
Our loyal customers benefit from our discount program. As you spend specific total sum in our service then you get a permanent discount up to 25%!
Stable servers
Our service has fast and stable servers with uptime close to 100%. We regulary monitor their status and solve any problems as soon as possible.
Professional support
Our support team has significant experiense with solving vpn connection technical problems. Such problems occur rare with our customers but if they do then we are here to help you.
No connection breaks
You can connect to our vpn even with an expired sub in order to write a ticket and fund your balance. At the moment when sub expires you don't get disconnected, opposite to other vpn services.
Many payment methods
With our service you can fund your balance with many methods such as popular online payment systems, banks and different cryptocurrencies.
Dedicated IPs
We offer dedicated IPs for rent so this IP will be used by you only. If you like to order a dedicated IP for your subscription then please contact our support team.
Принимаются
Perfect Money
мы принимаем
QIWI
мы принимаем
Яндекс деньги
bitcoin
СБЕРБАНК
ПриватБанк
liqpay.com
Альфа-Банк

Number 5

Revisiting the 7th edition of the National Intelligence Council's Global Trends report.

Five themes appear throughout this report and underpin this overall thesis.

1. First, shared **global challenges**—including climate change, disease, financial crises, and technology disruptions—are likely to manifest more frequently and intensely in almost every region and country.

These challenges—which often lack a direct human agent or perpetrator—will produce widespread strains on states and societies as well as shocks that could be catastrophic.

The ongoing COVID-19 pandemic marks the most significant, singular global disruption since World War II, with health, economic, political, and security implications that will ripple for years to come.

The effects of climate change and environmental degradation are likely to exacerbate food and water insecurity for poor countries, increase migration, precipitate new health challenges, and contribute to biodiversity losses.

Novel technologies will appear and diffuse faster and faster, disrupting jobs, industries, communities, the nature of power, and what it means to be human.

Continued pressure for global migration—as of 2020 more than 270 million persons were living in a country to which they have migrated, 100 million more than in 2000—will strain both origin and destination countries to manage the flow and effects.

These challenges will intersect and cascade, including in ways that are difficult to anticipate.

National security will require not only defending against armies and arsenals but also withstanding and adapting to these shared global challenges.

2. Second, the difficulty of addressing these transnational challenges is compounded in part by increasing **fragmentation** within communities, states, and the international system.

Paradoxically, as the world has grown more connected through communications technology, trade, and the movement of people, that very connectivity has divided and fragmented people and countries.

The hyperconnected information environment, greater urbanization, and interdependent economies mean that most aspects of daily life, including finances, health, and housing, will be more connected all the time.

The Internet of Things encompassed 10 billion devices in 2018 and is projected to reach 64 billion by 2025 and possibly many trillions by 2040, all monitored in real time.

In turn, this connectivity will help produce new efficiencies, conveniences, and advances in living standards.

However, it will also create and exacerbate tensions at all levels, from societies divided over core values and goals to regimes that employ digital repression to control populations.

As these connections deepen and spread, they are likely to grow increasingly fragmented along national, cultural, or political preferences.

In addition, people are likely to gravitate to information silos of people who share similar views, reinforcing beliefs and understanding of the truth.

Meanwhile, globalization is likely to endure but transform as economic and production networks shift and diversify.

All together, these forces portend a world that is both inextricably bound by connectivity and fragmenting in different directions.

3. The scale of transnational challenges, and the emerging implications of fragmentation, are exceeding the capacity of existing systems and structures, highlighting the third theme: **disequilibrium**.

There is an increasing mismatch at all levels between challenges and needs with the systems and organizations to deal with them.

The international system—including the organizations, alliances, rules, and norms—is poorly set up to address the compounding global challenges facing populations.

The COVID-19 pandemic has provided a stark example of the weaknesses in international coordination on health crises and the mismatch between existing institutions, funding levels, and future health challenges.

Within states and societies, there is likely to be a persistent and growing gap between what people demand and what governments and corporations can deliver.

From Beirut to Bogota to Brussels, people are increasingly taking to the streets to express their dissatisfaction with governments' ability to meet a wide range of needs, agendas, and expectations.

As a result of these disequilibriums, old orders—from institutions to norms to types of governance—are strained and in some cases, eroding. And actors at every level are struggling to agree on new models for how to structure civilization.

4. A key consequence of greater imbalance is greater **contestation** within communities, states, and the international community.

This encompasses rising tensions, division, and competition in societies, states, and at the international level.

Many societies are increasingly divided among identity affiliations and at risk of greater fracturing.

Relationships between societies and governments will be under persistent strain as states struggle to meet rising demands from populations.

As a result, politics within states are likely to grow more volatile and contentious, and no region, ideology, or governance system seems immune or to have the answers.

At the international level, the geopolitical environment will be more competitive—shaped by China's challenge to the United States and Western-led international system. Major powers are jockeying to establish and exploit new rules of the road.

This contestation is playing out across domains from information and the media to trade and technological innovations.

5. Finally, **adaptation** will be both an imperative and a key source of advantage for all actors in this world.

Climate change, for example, will force almost all states and societies to adapt to a warmer planet.

Some measures are as inexpensive and simple as restoring mangrove forests or increasing rainwater storage; others are as complex as building massive sea walls and planning for the relocation of large populations.

Demographic shifts will also require widespread adaption.

Countries with highly aged populations like China, Japan, and South Korea, as well as Europe, will face constraints on economic growth in the absence of adaptive strategies, such as automation and increased immigration.

Technology will be a key avenue for gaining advantages through adaptation.

For example, countries that are able to harness productivity boosts from artificial intelligence (AI) will have expanded economic opportunities that could allow governments to deliver more services, reduce national debt, finance some of the costs of an aging population, and help some emerging countries avoid the middle-income trap.

The benefits from technology like AI will be unevenly distributed within and between states, and more broadly, adaptation is likely to reveal and exacerbate inequalities.

The most effective states are likely to be those that can build societal consensus and trust toward collective action on adaptation and harness the relative expertise, capabilities, and relationships of nonstate actors to complement state capacity.

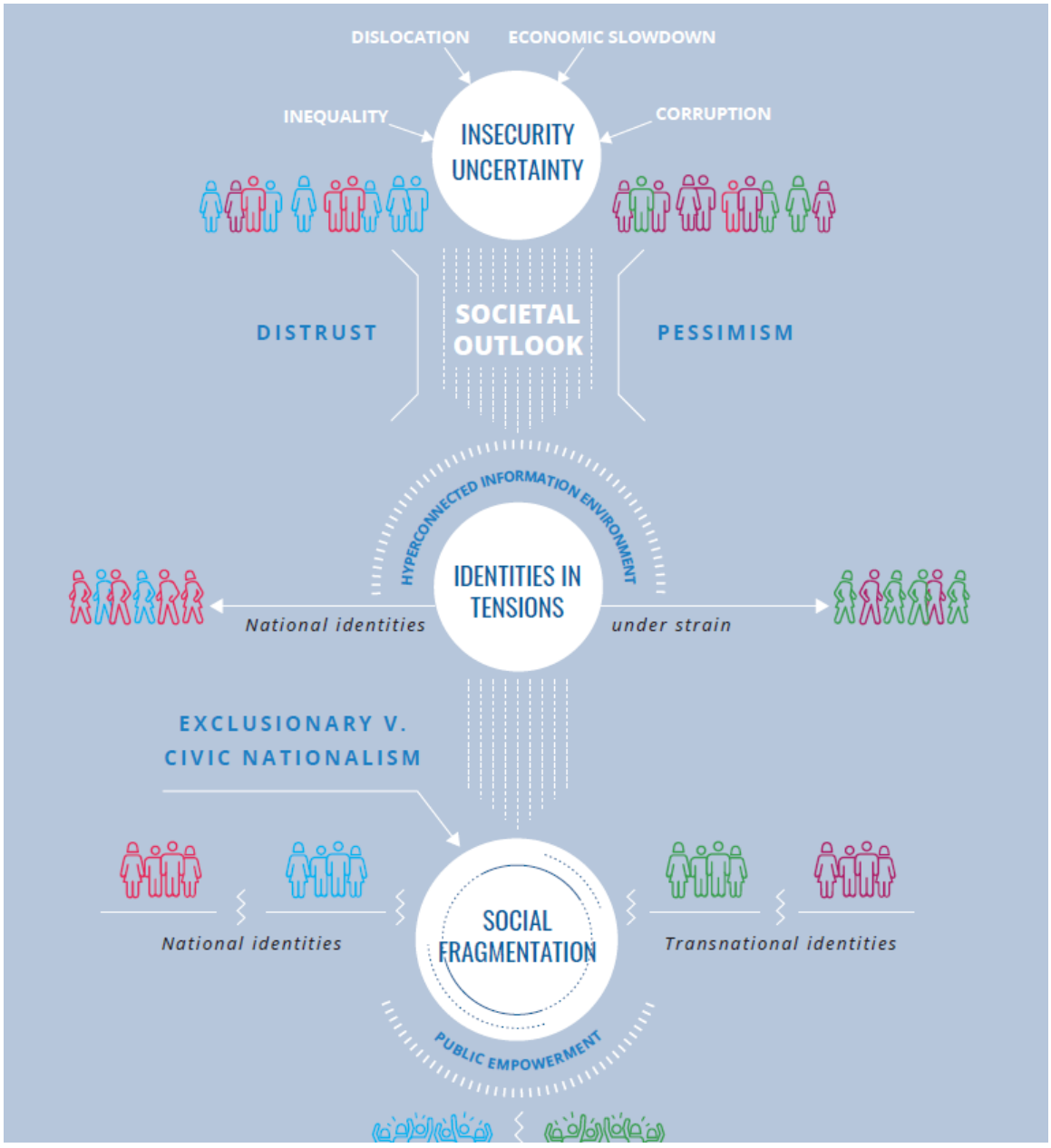
To read more: https://www.dni.gov/index.php/gt2040-home

Number 6

National Intelligence Council's Global Trends report.

Emerging Dynamics

Societal:Disillusioned, informed, and divided



Key Takeaways

- Slowing economic growth and gains in human development, coupled with rapid societal changes, have left large segments of the global

population feeling insecure, uncertain about the future, and distrustful of institutions and governments they view as corrupt or ineffective.

- Many people are gravitating toward familiar and like-minded groups for community and security, including ethnic, religious, and cultural identities as well as groupings around interests and causes. These groups are more prominent and in conflict, creating a cacophony of competing visions, goals, and beliefs.

- The combination of newly prominent transnational identities, the resurgence of established allegiances, and a siloed information environment is creating and exposing fault lines within states, undermining civic nationalism, and increasing volatility.

- Populations in every region are becoming better equipped with the tools, capacity, and incentive to agitate for social and political change and to demand resources, services, and recognition from their governments.

RISING PESSIMISM, WAVERING TRUST

Global and local challenges, including economic strains, demographic shifts, extreme weather events, and rapid technological change, are increasing perceptions of physical and social insecurity for much of the world's population.

The COVID-19 pandemic is intensifying these economic and social challenges. Many people, particularly those who are benefiting less than others in their societies, are increasingly pessimistic about their own prospects, frustrated with government performance, and believe governments are favoring elites or pursuing the wrong policies.

The economic growth and rapid improvements in health, education, and human development of the past few decades have begun to level off in some regions, and people are sensitive to the increasing gap between winners and losers in the globalized economy and are seeking redress from their governments.

Approximately 1.5 billion people moved up into the middle class in the past few decades, but some are beginning to fall back, including in advanced economies.

Public opinion polls repeatedly have shown increasing pessimism about the future in countries of all types around the world, but especially in advanced and middle-income economies.

According to the 2020 Edelman Trust Barometer, the majority of respondents in 15 of 28 countries polled are pessimistic that they and their families will be better off in five years, an average increase of 5 percent from the previous year.

Less than a quarter of those polled in France, Germany, and Japan, for example, believe they will be better off in 2025.

In coming years, this pessimism is likely to spread in developing countries with large youthful populations but with slowing progress in eradicating poverty and meeting human development needs, particularly Sub-Saharan Africa.

Potentially slower economic growth in coming years and smaller gains in human development in many countries are likely to exacerbate distrust of institutions and formal sources of authority for some members of the public.

Trust in governments and institutions, which is highly dependent on perceptions of fairness and effectiveness, has been consistently low for the past decade, particularly in middle- to high-income countries.

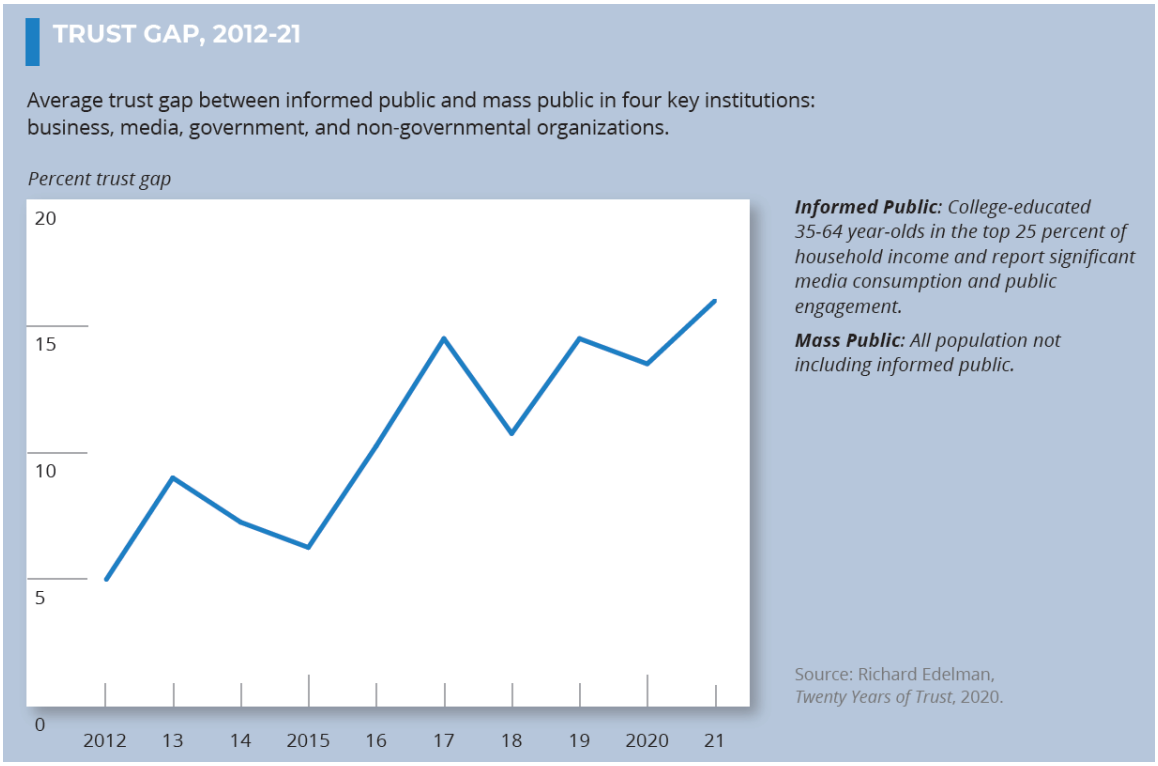
In a 2020 study of 16 developed countries by Edelman, the portion of the mass public trusting government since 2012 never exceeded 45 percent, and among Organization for Economic Cooperation and Development (OECD) economies, public trust in government fell in more than half of countries between 2006 and 2016, according to separate public opinion polling by Gallup.

Of 11 geographically diverse countries analyzed by Edelman during the COVID-19 pandemic, public trust in government increased an average of 6 percentage points between January and May 2020, and then it declined an average of 5 percentage points between May 2020 and January 2021 as governments failed to contain the coronavirus.

Trust is not uniform across societies. Globally, trust in institutions among the informed public—defined as people who are college educated, are in the top 25 percent of household income in each market, and exhibit significant media consumption—has risen during the past 20 years whereas more than half of the mass public during the past decade repeatedly say the “system” is failing them.

The gap in trust in institutions between the informed public and the mass public has increased during the past decade, according to the Edelman surveys, showing a gap of 5 percentage points in 2012 and 16 points in the

2021 report. Similarly, the gap in trust in business quadrupled during this period.



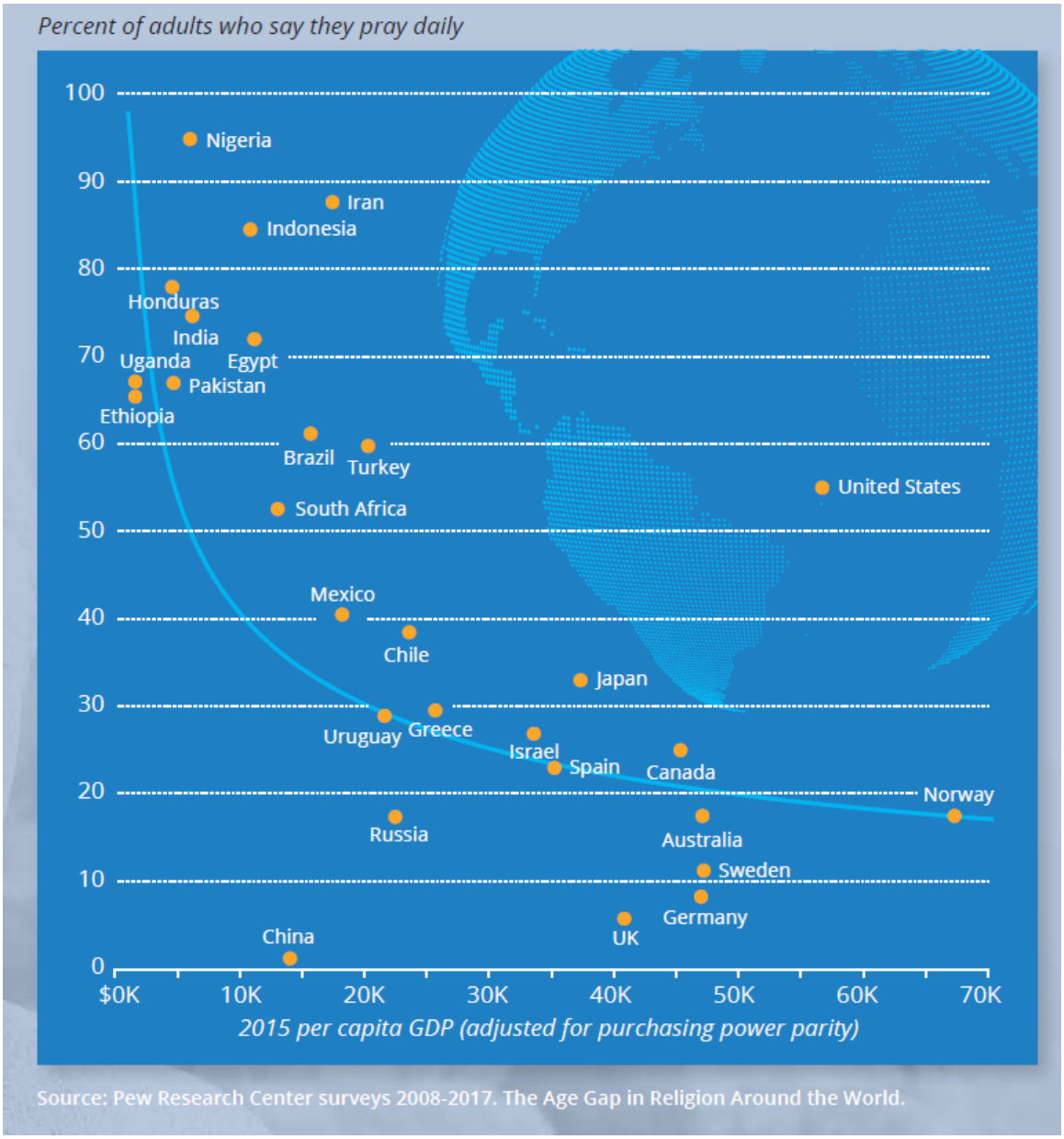
Increasing actual or perceived inequality within countries, particularly in those in which overall economic growth is slowing, often coincides with declining trust and rising public dissatisfaction with the political system.

In less developed countries, corruption is undermining confidence in government, and people tend to trust informal institutions more than government where political power is concentrated among the wealthy elite.

Corruption is now one of the most dominant factors driving demand for political change.

According to 2019 polling by Transparency International, a majority of respondents across Latin America (53 percent), the Middle East and North Africa (65 percent), and Sub-Saharan Africa (55 percent) said that corruption is increasing in their region.

In coming years, advancements in artificial intelligence (AI), machine learning, 5G, and other technologies that will expand access to the Internet could further diminish public trust as people struggle to determine what is real and what is rumor or manipulation.
In addition, populations fear the increasingly pervasive surveillance and monitoring by governments and fear private corporations seeking control or profit from their personal information.



IDENTITIES MORE PROMINENT

As trust in governments, elites, and other established institutions erodes, societies are likely to fragment further based on identities and beliefs.

People in every region are turning to familiar and like-minded groups for community and a sense of security, including cultural and other subnational identities as well as transnational groupings and interests. Identities and affiliations are simultaneously proliferating and becoming more pronounced. In turn, this is leading to more influential roles for identity groups in societal and political dynamics but also generating divisions and contention.

Many people are gravitating to more established identities, such as ethnicity and nationalism. In some countries, slowing population growth, increasing migration, and other demographic shifts are intensifying perceptions of vulnerability, including a sense of cultural loss.

Many people who feel displaced by rapid social and economic changes resent violations of age-old traditions and perceive that others are benefiting from the system at their expense. These perceptions also fuel beliefs that economic and social change is damaging and that some leaders are pursuing misguided goals.

Consistent with the growing salience of established identities, religion continues to play important roles in people's lives, shaping what they believe, whom they trust, with whom they congregate, and how they engage publicly.

In developing regions where populations are growing fastest, including Africa, South Asia, and parts of Latin America, publics report greater participation in religious practices, pointing to the sense of purpose religion provides. Perceptions of existential threats from conflict, disease, or other factors also contribute to higher levels of religiosity.

To read more: https://www.dni.gov/index.php/gt2040-home

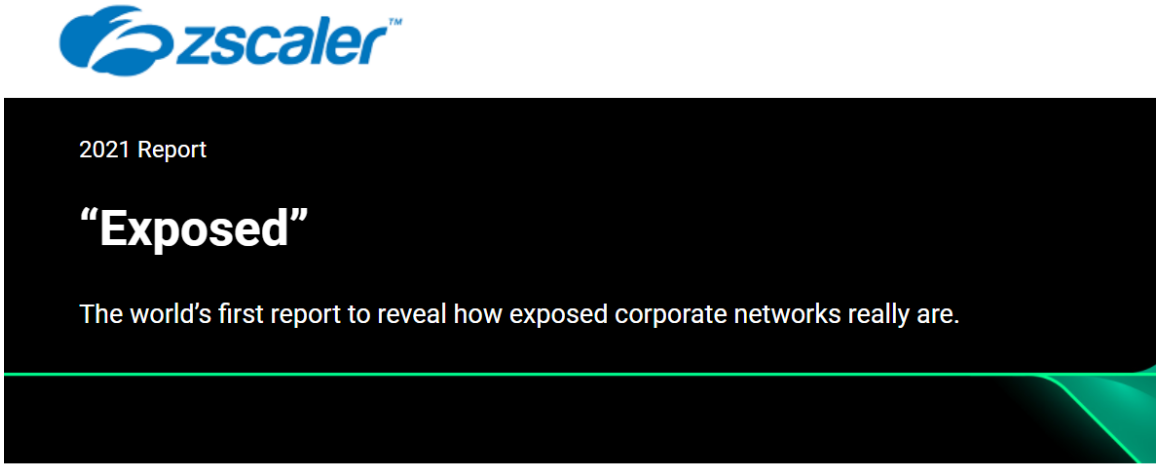
Number 7

Unsecured servers and cloud services leave networks exposed to cyber attacks

National Cyber Security Centre

New Analysis by Zscaler of 1500 corporate networks found exposed servers, ports and cloud services in the hundreds of thousands.

The research also found over 200,000 unpatched common vulnerabilities and exposures (CVEs), of which almost half were classed as “Critical” or “High” severity. You may visit: https://info.zscaler.com/resources-ebooks-global-corporate-network-attack-surface-report



*This report provides, “…**a first-ever look at the possible impact on attack surface due to remote work during the global pandemic.**”*
– “Exposed” Report, 2021

Securing your users, devices, and applications has become difficult with the rise in remote work—especially with most business now being done over the internet. On one hand, cloud and mobility have allowed you to scale, but they’ve also created a significant attack surface as cybercriminals target users and remote access VPNs. To reduce this risk, IT leaders must minimize network exposure to the internet.

The expansion in use of cloud services to support working outside of the usual corporate networks, as a result of the coronavirus pandemic, has given cyber criminals an increased attack surface. Unpatched vulnerabilities and unsecured networks can be exploited by malicious users for identity theft, data theft, ransomware or other malware activities.

The NCSC has produced guidance to help organisations better understand securely setting up homeworking and moving businesses online from a physical environment.

We also always recommend making sure that your data is backed up and crucially that security patches are applied as soon as is practicable. Advice on assessing and prioritising vulnerabilities may help with your patching regime.

You may visit: https://www.ncsc.gov.uk/report/weekly-threat-report-25th-june-2021

Number 8

A new notice in Search for rapidly evolving results

Danny Sullivan, Public Liaison for Search

Google

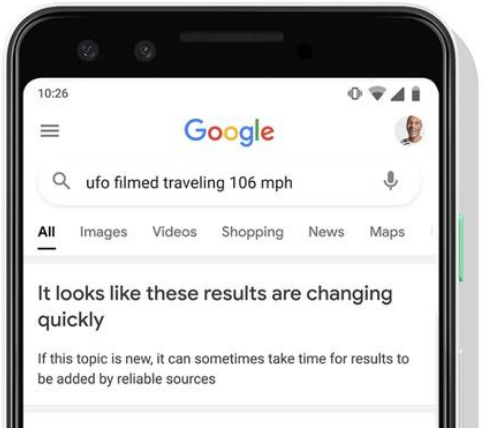
Accessing timely, relevant and reliable information is increasingly important in our current environment. Whether you see something on social media or are having a conversation with a friend, you might turn to Google to learn more about a developing issue.

While Google Search will always be there with the most useful results we can provide, sometimes the reliable information you're searching for just isn't online yet.

This can be particularly true for breaking news or emerging topics, when the information that's published first may not be the most reliable.

To help with this, we've trained our systems to detect when a topic is rapidly evolving and a range of sources hasn't yet weighed in.

We'll now show a notice indicating that it may be best to check back later when more information from a wider range of sources might be available.



Since last year, we've had similar notices that let you know when Google hasn't been able to find anything that matches your search particularly well.

With our recently-launched About This Result panel, you can also quickly find information about sources you find on Google Search and better determine if they're likely to provide helpful or trustworthy information.

With this additional context, you can make a more informed decision about the sites you may want to visit and what results will be most useful for you.

Across these features, our goal is to provide more context about your results so you can more confidently evaluate the information you find online.

These new notices are rolling out in English in the U.S. to start, and we look forward to expanding these and other related features over the coming months.

Number 9

NIST Method Uses Radio Signals to Image Hidden and Speeding Objects

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Researchers at the National Institute of Standards and Technology (NIST) and Wavsens LLC have developed a method for using radio signals to create real-time images and videos of hidden and moving objects, which could help firefighters find escape routes or victims inside buildings filled with fire and smoke. The technique could also help track hypersonic objects such as missiles and space debris.

The new method, described June 25 in Nature Communications, could provide critical information to help reduce deaths and injuries. Locating and tracking first responders indoors is a prime goal for the public safety community. Hundreds of thousands of pieces of orbiting space junk are considered dangerous to humans and spacecraft.

“Our system allows real-time imaging around corners and through walls and tracking of fast-moving objects such as millimeter-sized space debris flying at 10 kilometers per second, more than 20,000 miles per hour, all from standoff distances,” said physicist Fabio da Silva, who led the development of the system while working at NIST.

“Because we use radio signals, they go through almost everything, like concrete, drywall, wood and glass,” da Silva added. “It’s pretty cool because not only can we look behind walls, but it takes only a few microseconds of data to make an image frame. The sampling happens at the speed of light, as fast as physically possible.”

The NIST imaging method is a variation on radar, which sends an electromagnetic pulse, waits for the reflections, and measures the round-trip time to determine distance to a target. Multisite radar usually has one transmitter and several receivers that receive echoes and triangulate them to locate an object.

“We exploited the multisite radar concept but in our case use lots of transmitters and one receiver,” da Silva said. “That way, anything that reflects anywhere in space, we are able to locate and image.”

Da Silva has applied for a patent, and he recently left NIST to commercialize the system under the name m-Widar (microwave image detection, analysis and ranging) through a startup company, Wavsens LLC (Westminster, Colorado).

The NIST team demonstrated the technique in an anechoic (non-echoing) chamber, making images of a 3D scene involving a person moving behind drywall. The transmitter power was equivalent to 12 cellphones sending signals simultaneously to create images of the target from a distance of about 10 meters (30 feet) through the wallboard.

Da Silva said the current system has a potential range of up to several kilometers. With some improvements the range could be much farther, limited only by transmitter power and receiver sensitivity, he said.

The basic technique is a form of computational imaging known as transient rendering, which has been around as an image reconstruction tool since 2008. The idea is to use a small sample of signal measurements to reconstruct images based on random patterns and correlations. The technique has previously been used in communications coding and network management, machine learning and some advanced forms of imaging.

Da Silva combined signal processing and modeling techniques from other fields to create a new mathematical formula to reconstruct images. Each transmitter emits different pulse patterns simultaneously, in a specific type of random sequence, which interfere in space and time with the pulses from the other transmitters and produce enough information to build an image.

The transmitting antennas operated at frequencies from 200 megahertz to 10 gigahertz, roughly the upper half of the radio spectrum, which includes microwaves. The receiver consisted of two antennas connected to a signal digitizer. The digitized data were transferred to a laptop computer and uploaded to the graphics processing unit to reconstruct the images.

The NIST team used the method to reconstruct a scene with 1.5 billion samples per second, a corresponding image frame rate of 366 kilohertz (frames per second). By comparison, this is about 100 to 1,000 times more frames per second than a cellphone video camera.

With 12 antennas, the NIST system generated 4096-pixel images, with a resolution of about 10 centimeters across a 10-meter scene. This image resolution can be useful when sensitivity or privacy is a concern. However, the resolution could be improved by upgrading the system using existing technology, including more transmitting antennas and faster random signal generators and digitizers.

In the future, the images could be improved by using quantum entanglement, in which the properties of individual radio signals would become interlinked. Entanglement can improve sensitivity. Radio-

frequency quantum illumination schemes could increase reception sensitivity.

The new imaging technique could also be adapted to transmit visible light instead of radio signals — ultrafast lasers could boost image resolution but would lose the capability to penetrate walls — or sound waves used for sonar and ultrasound imaging applications.

In addition to imaging of emergency conditions and space debris, the new method might also be used to measure the velocity of shock waves, a key metric for evaluating explosives, and to monitor vital signs such as heart rate and respiration, da Silva said.

This work was funded in part by the Public Safety Trust Fund, which provides funding to organizations across NIST leveraging NIST expertise in communications, cybersecurity, manufacturing and sensors for research on critical, lifesaving technologies for first responders.

Da Silva explains the imaging process like this: To image a building, the actual volume of interest is much smaller than the volume of the building itself because it's mostly empty space with sparse stuff in it. To locate a person, you would divide the building into a matrix of cubes. Ordinarily, you would transmit radio signals to each cube individually and analyze the reflections, which is very time consuming. By contrast, the NIST method probes all cubes at the same time and uses the return echo from, say, 10 out of 100 cubes to calculate where the person is. All transmissions will return an image, with the signals forming a pattern and the empty cubes dropping out.

Number 10

BIS Annual Economic Report

BIS

Introduction

It is now over a year since the Covid-19 pandemic struck out of the blue, plunging the global economy into a historically deep recession.

An acute health crisis turned into an overwhelming economic crisis, as policymakers adopted stringent containment measures to save lives.

This was a recession in response to an insidious invisible enemy.

A timely, forceful and concerted policy drive prevented the worst. Working together, monetary, fiscal and prudential authorities managed to stabilise the financial system and cushion the blow. They put the patient in a state of suspended animation.

But as last year's Annual Economic Report (AER) went to press, uncertainty still reigned: what would happen next? There was hardly any precedent to serve as a benchmark. No recent pandemic was remotely as damaging as the current one.

And the Spanish flu outbreak was too distant and too different. Many central banks suspended publishing forecasts, turning to tentative scenarios instead.

Where do we stand today? We know much more about the enemy and we are better equipped to fight it. We know much more about how the economy responds and how far it can adjust.

The patient is in much better health but has not yet fully recovered. Some parts of the body are in better shape than others. What is clear is that the recovery will be uneven and the long-term consequences material.

"Pandexit" will be bumpy and leave a costly and long-lasting legacy.

How has the global economy fared during the past year? What are the prospects and risks? What are the policy challenges?

While central banks were tackling the consequences of the pandemic, other important issues continued to draw attention.

Questions pertaining to the relationship between monetary policy and inequality moved to the centre of public discourse.

In addition, discussion and analysis of central bank digital currencies (CBDCs) became livelier than ever.

What follows elaborates on these issues.

A surprisingly strong but very uneven recovery

Starting in the second half of 2020, the global economy rebounded more strongly than anticipated.

Private consumption was the main engine of growth.

As Covid-19 broke out, there had been widespread concerns about "scarring effects" on consumers' spending.

It had been feared that lingering risk aversion and contagion worries would hold it back. In the event, these fears proved unfounded.

The craving for normality prevailed.

Whenever containment measures were relaxed in contactintensive services, demand returned swiftly.

In addition, as consumers adapted, a further shift to e-commerce limited the restrictions' fallout.

At the same time, rates of change should not be confused with levels. For the year as a whole, GDP still declined by some 3.4%.

To be sure, at the time of writing world GDP has more or less returned to its pre-crisis level. But this masks a clear divide between China, where GDP is now well above its pre-crisis level, and the rest of the world, where it is still generally some way below.

To read more: https://www.bis.org/publ/arpdf/ar2021e.pdf

Number II

Phishing most common Cyber Incident faced by SMEs

The European Union Agency for Cybersecurity identifies the cybersecurity challenges SMEs face today and issues recommendations.

Small and medium-sized enterprises (SMEs) are considered to be the backbone of Europe's economy. 25 millions of SMEs are active today in the European Union and employ more than 100 million workers.

The report Cybersecurity for SMEs ENISA issues today provides advice for SMEs to successfully cope with cybersecurity challenges, particularly those resulting from the COVID-19 pandemic.

With the current crisis, traditional businesses had to resort to technologies such as QR codes or contactless payments they had never used before.

Although SMEs have turned to such new technologies to maintain their business, they often failed to increase their security in relation to these new systems.
Research and real-life experience show that well prepared organisations deal with cyber incidents in a much more efficient way than those failing to plan or lacking the capabilities they need to address cyber threats correctly.

Juhan Lepassaar, EU Agency for Cybersecurity Executive Director said: "SMEs cybersecurity and support is at the forefront of the EU's cybersecurity strategy for the digital decade and the Agency is fully dedicated to support the SME community in improving their resilience to successfully transform digitally."

In addition to the report, ENISA also publishes today the Cybersecurity Guide for SMEs: "12 steps to securing your business". The short cybersecurity guide provides SMEs with practical high-level actions to better secure their systems, hence their businesses.

Based on an extended desktop research, an extensive survey and targeted interviews, the report identifies those pre-existing cybersecurity challenges worsened by the impact of the pandemic crisis.

Key findings

85% of the SMEs surveyed agree that cybersecurity issues would have a serious detrimental impact on their businesses with 57% saying they would most likely go out of business.

Out of almost 250 SMEs surveyed, 36% reported that they had experienced an incident in the last 5 years. Nonetheless, cyberattacks are still not considered as a major risk for a large number of SMEs and a belief remains that cyber incidents are only targeting larger organisations.

However, the study reveals that phishing attacks are among the most common cyber incidents SMEs are likely to be exposed to, in addition to ransomware attacks, stolen laptops, and Chief Executive Officer (CEO) frauds.

For instance, with the concerns induced by the pandemic, cyber criminals seek to compromise accounts using phishing emails with Covid-19 as a subject.

CEO frauds are other decoys meant to lure an employee into acting upon the instructions of a fraudulent email displayed as if sent from their CEO, and usually requesting a payment to be performed in urgency under business-like circumstances.

The report unveils the following challenges SMEs are faced with:

- Low awareness of cyber threats;
- Inadequate protection for critical and sensitive information;
- Lack of budget to cover costs incurred for implementing cybersecurity measures;

- Availability of ICT cybersecurity expertise and personnel;
- Absence of suitable guidelines tailored to the SMEs sector;
- Moving online;
- Low management support.

How to address those challenges?

The recommendations issued fall into three categories:

People

People play an essential role in the cybersecurity ecosystem. The report draws attention to the importance of responsibility, employee buy-in and awareness, cybersecurity training and cybersecurity policies as well as third party management in relation to confidential and/or sensitive information.

Processes

Monitoring internal business processes include performing audits, incident planning and response, passwords, software patches and data protection.

Technical

At the technical level, a number of aspects should be considered in relation to network security, anti-virus, encryption, security monitoring, physical security and the securing of backups.

Number 12

Data of 700 million LinkedIn users reportedly advertised on dark web

National Cyber Security Centre

Data belonging to 700 million LinkedIn users has reportedly been advertised for sale on the dark web.

Based on a sample data set, security researchers found information relating to real accounts including users' full names, email addresses, phone numbers and physical addresses.

LinkedIn has posted an update about the reports, stating that this is not a data breach and its initial investigations have found the information was scraped from the internet. It said no private Linkedin member data had been exposed. You may visit: https://news.linkedin.com/2021/june/an-update-from-linkedin

Affected LinkedIn users should still be vigilant against suspicious messages and phone calls relating to their scraped data. Cyber criminals are opportunistic and may use the recent news to trick people into clicking on scam messages.

The NCSC has produced guidance to help individuals spot suspicious messages and deal with them effectively, and more relevant advice on actions to take can be found in our data breaches guidance.

An update on report of scraped data

LinkedIn Pressroom

Our teams have investigated a set of alleged LinkedIn data that has been posted for sale. We want to be clear that this is not a data breach and no private LinkedIn member data was exposed.

Our initial investigation has found that this data was scraped from LinkedIn and other various websites and includes the same data reported earlier this year in our April 2021 scraping update.

Members trust LinkedIn with their data, and any misuse of our members' data, such as scraping, violates LinkedIn terms of service. When anyone tries to take member data and use it for purposes LinkedIn and our members haven't agreed to, we work to stop them and hold them accountable.

For additional information about our policies and how we protect member data from misuse:
https://www.linkedin.com/help/linkedin/answer/56347/prohibited-software-and-extensions

Number 13

Thousands of fake online pharmacies shut down in INTERPOL operation

A record number of fake online pharmacies have been shut down under Operation Pangea XIV targeting the sale of counterfeit and illicit medicines and medical products.

The operation coordinated by INTERPOL involved police, customs and health regulatory authorities from 92 countries.

It resulted in 113,020 web links including websites and online marketplaces being closed down or removed, the highest number since the first Operation Pangea in 2008.

In Venezuela a man was arrested after he developed an e-commerce platform on WhatsApp to sell illicit medicines.

In the UK, in addition to the seizure of some three million fake medicines and devices worth more than USD 13 million, authorities also removed more than 3,100 advertising links for the illegal sale and supply of unlicensed medicines, and shut down 43 websites.

Operation Pangea XIV also showed that criminals are continuing to cash in on the demand for personal protection and hygiene products generated by the COVID-19 pandemic.

Fake and unauthorized COVID-19 testing kits accounted for more than half of all medical devices seized during the week of action (18 – 25 May) which resulted in 277 arrests worldwide and the seizure of potentially dangerous pharmaceuticals worth more than USD 23 million.

In Italy, authorities recovered more than 500,000 fake surgical masks as well as 35 industrial machines used for production and packaging.

"As the pandemic forced more people to move their lives online, criminals were quick to target these new 'customers'," said INTERPOL Secretary General Jürgen Stock.

"Whilst some individuals were knowingly buying illicit medicines, many thousands of victims were unwittingly putting their health and potentially their lives at risk.

"The online sale of illicit medicines continues to pose a threat to public safety, which is why operations such as Pangea remain vital in combating this global health scourge," added Secretary General Stock.

"As crimes continue to evolve amidst the COVID-19 pandemic, the authorities must remain vigilant in dismantling criminal networks involved in the proliferation of illicit pharmaceutical products especially in online platforms," said the Head of the INTERPOL National Central Bureau in the Philippines, Allan C. Guisihan.

"Despite the official conclusion of this operation, the Philippines will continue to pursue its efforts in protecting the environment to ensure public health."

"Through Operation Pangea, we have supported INTERPOL, the UK's Medicines and Healthcare products Regulatory Agency and Border Force in tackling the worldwide threat of pharmaceutical crime linked to the COVID-19 pandemic.

We have seen how organized crime groups have responded to the changing environment however, we also continue to adapt and work with partners to disrupt their activities," said Kathryn Clarke Head of UK International Crime Bureau from the National Crime Agency.

Checks of some 710,000 packages led to the discovery of fake and illicit drugs hidden amongst legitimate products including clothes, jewellery, toys, food and baby products. In Qatar officials discovered 2,805 nerve pain tablets hidden inside tins of baked beans.

Supported by the Pharmaceutical Security Institute, the United Nations Office on Drugs and Crime/World Customs Organization's Container Control Programme and Europol, overall the operation resulted in the seizure of around 9 million medical devices and illicit pharmaceuticals, including:

- Hypnotic and sedative medication
- erectile dysfunction pills
- Medical devices (Covid Test kits, masks, syringes, catheters, surgical devices etc)
- analgesics/painkillers
- anabolic steroids
- antiseptics and germicides
- anti-cancer medication
- anti-malarials
- vitamins

To read more: https://www.interpol.int/en/News-and-Events/News/2021/Thousands-of-fake-online-pharmacies-shut-down-in-INTERPOL-operation

Number 14

Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments

Executive summary

Since at least mid-2019 through early 2021, Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165, used a Kubernetes cluster to conduct widespread, distributed, and anonymized brute force access attempts against hundreds of government and private sector targets worldwide.

GTsSS malicious cyber activity has previously been attributed by the private sector using the names Fancy Bear, APT28, Strontium, and a variety of other identifiers.

The 85th GTsSS directed a significant amount of this activity at organizations using Microsoft Office 365 cloud services; however, they also targeted other service providers and onpremises email servers using a variety of different protocols.

These efforts are almost certainly still ongoing.

This brute force capability allows the 85th GTsSS actors to access protected data, including email, and identify valid account credentials. Those credentials may then be used for a variety of purposes, including initial access, persistence, privilege escalation, and defense evasion.

The actors have used identified account credentials in conjunction with exploiting publicly known vulnerabilities, such as exploiting Microsoft Exchange servers using CVE 2020-0688 and CVE 2020-17144, for remote code execution and further access to target networks.

After gaining remote access, many well-known tactics, techniques, and procedures (TTPs) are combined to move laterally, evade defenses, and collect additional information within target networks.

Network managers should adopt and expand usage of multi-factor authentication to help counter the effectiveness of this capability. Additional mitigations to ensure strong access controls include time-out and lock-out features, the mandatory use of strong passwords, implementation of a Zero Trust security model that uses additional

attributes when determining access, and analytics to detect anomalous accesses.

Additionally, organizations can consider denying all inbound activity from known anonymization services, such as commercial virtual private networks (VPNs) and The Onion Router (TOR), where such access is not associated with typical use.

Description of targets

This campaign has already targeted hundreds of U.S. and foreign organizations worldwide, including U.S. government and Department of Defense entities. While the sum of the targeting is global in nature, the capability has predominantly focused on entities in the U.S. and Europe.

Types of targeted organizations include:

Known TTPs

The actors used a combination of known TTPs in addition to their password spray operations to exploit target networks, access additional credentials, move laterally, and collect, stage, and exfiltrate data, as illustrated in the figure below. The actors used a variety of protocols,

including HTTP(S), IMAP(S), POP3, and NTLM. The actors also utilized different combinations of defense evasion TTPs in an attempt to disguise some components of their operations; however, many detection opportunities remain viable to identify the malicious activity.

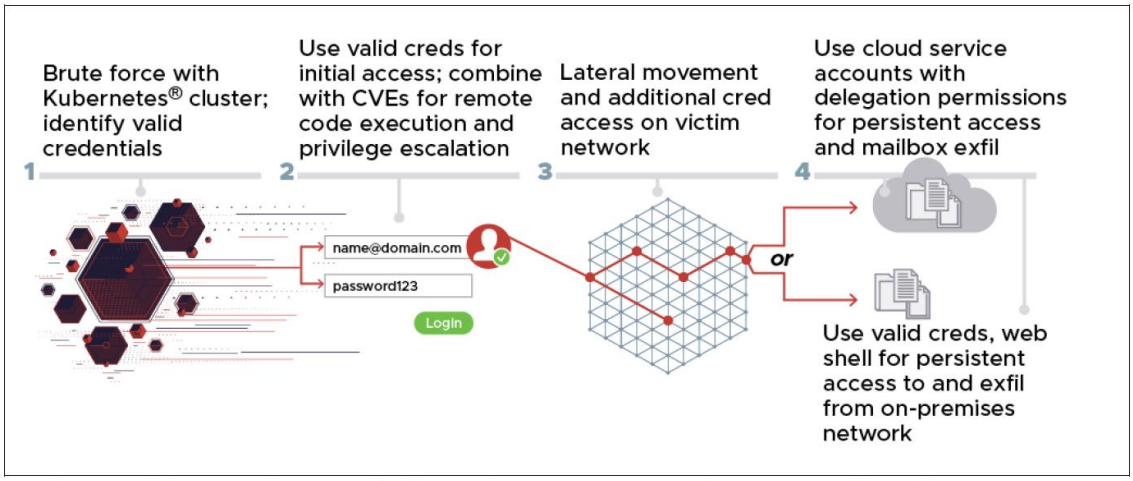


Figure 1: Example of several TTPs used together as part of this type of brute force campaign

To read more: https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn and Facebook pages of Cyber Risk GmbH.

Readers will make their own determination of how suitable the information is for their usage and intent. Cyber Risk GmbH expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

Cyber Risk GmbH and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. Cyber Risk GmbH does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of interpretative;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.