International Association of Risk and Compliance Professionals (IARCP)
1200 G Street NW Suite 800, Washington DC, 20005-6705 USA
Tel: 202-449-9750, Web: www.risk-compliance-association.com

Monday, July 5, 2021

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

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. Welcome to our Top 10 list.

Best regards,

George Lekatis
President of the IARCP
1200 G Street NW Suite 800,
Washington DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington DE 19801, USA
Tel: (302) 342-8828

Number 1 (Page 1)

Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships

Overview of responses to the public consultation

Number 2 (Page 1)

Insurance stress test 2021

Prolonged COVID-19 scenario in a “lower for longer” interest rate environment

Number 3 (Page 1)

Artificial Intelligence Governance Principles: Towards ethical and trustworthy artificial intelligence in the European Insurance sector.

A report from EIOPA´s Consultative Expert Group on Digital Ethics in insurance

Number 4 (Page 1)

Opportunities and risks of central bank digital currencies

Burkhard Balz, Member of the Executive Board of the Deutsche Bundesbank, at the virtual European Payments Conference "Key Trends in the European Payments Landscape".

Number 5 (Page 1)

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

Number 6 (Page 1)

National Intelligence Council's Global Trends report.

Emerging Dynamics
Societal:Disillusioned, informed, and divided

Number 7 (Page 1)

Competition and collaboration: Understanding interacting epidemics can unlock better disease forecasts

By Andrey Lokhov

Number 8 (Page 1)

Cyber Security in a changing and complex world

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

Number 9 (Page 1)

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 10 (Page 1)

Developing Morphogenic Electrochemical Interfaces

Advanced math modeling to enable new designs for persistent batteries, anti-corrosion coatings

Number 1

Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships

Overview of responses to the public consultation

FSB FINANCIAL STABILITY BOARD

On 9 November 2020, the Financial Stability Board (FSB) published a discussion paper for public consultation on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships.

The discussion paper drew on findings from a survey conducted among FSB members, and identified a number of issues and challenges.

To facilitate and inform discussions among authorities (including supervisory and resolution authorities), financial institutions and third parties on how to address the issues identified, the discussion paper invited comments from external stakeholders on:

1. the key challenges in identifying, managing and mitigating the risks relating to outsourcing and third-party relationships (including risks in sub-contractors and the broader supply chain);

2. possible ways to address these challenges and mitigate related risks, including in a cross-border context; and

3. lessons learnt from COVID-19 relating to outsourcing and third-party relationships.

The public consultation period for the discussion paper ended on 8 January 2021. The FSB received 39 responses from a wide range of stakeholders including banks, insurers, asset managers, financial market infrastructures (FMIs), third-party service providers, industry associations, individuals and public authorities.

The FSB also held a virtual outreach meeting in late February 2021 to discuss: evolving industry practices; practical challenges associated with outsourcing and third-party risk management; and potential ways to improve coordination among the relevant stakeholders (i.e. supervisory and resolution authorities, financial institutions and third-party service providers) with a view to enhancing the resilience of financial institutions and the financial system.

Respondents generally welcomed the discussion paper, which they viewed as a timely and balanced overview of the benefits and challenges relating to the evolving nature of financial institutions' outsourcing and third-party dependencies.

Respondents agreed with the challenges and issues identified in the discussion paper, such as: constraints on the rights to access, audit and obtain information from third parties; and concentration risks in the provision of certain critical services that are very difficult to substitute.

In addition, treatment of intra-group outsourcing, fragmentation of regulatory, supervisory and industry practices across sectors and borders, restrictive data localisation requirements, cyber and data security, and resource constrains at financial institutions as well as supervisory authorities were highlighted as potential challenges or issues that deserve attention.

To address these challenges or issues, respondents suggested a range of measures that can be categorised into five areas:

(i) the development of global standards on outsourcing and thirdparty risk management;

(ii) the adoption of consistent definitions and terminology;

(iii) pooled audits, certificates and reports;

(iv) dependency mapping and enhanced supervisory oversight; as well as

(v) enhanced cross-border cooperation and dialogue with stakeholders.

This note summarises the main issues raised and views expressed in the public consultation, including the virtual outreach meeting (which are not necessarily shared and endorsed by FSB members).

To read more: https://www.fsb.org/wp-content/uploads/P140621.pdf

Number 2

Insurance stress test 2021

Prolonged COVID-19 scenario in a "lower for longer" interest rate environment

EIOPA carries out regular insurance stress tests to assess how well the European insurance industry is able to cope with severe but plausible adverse development of the financial and economic conditions.

Stress test results help supervisors identify the vulnerabilities of the insurance industry and how to improve its resilience.

The 2021 stress test exercise focuses on a prolonged COVID-19 scenario in a "lower for longer" interest rate environment and evaluates its impacts on the capital and liquidity position of the entities in scope.

Objective

The 2021 stress test exercise aims to assess the resilience of the participants to the adverse scenario(s) by a capital and liquidity perspective in order to provide supervisors with information on whether these insurers are able to withstand severe but plausible shocks.

While not being a pass/fail exercise, the 2021 exercise has mainly a microprudential approach. It allows EIOPA to make recommendations to the industry and enables supervisors to ask insurance undertakings to take remedial actions, when needed, in order to improve their resilience.

The microprudential assessment is complemented by the estimation of potential spill-over from the insurance sector triggered by widespread reactions to the prescribed shocks.

Scenario

The 2021 stress test exercise focuses on a prolonged COVID-19 scenario in a "lower for longer" interest rate environment.

The scenario, developed in cooperation with the ESRB, elaborates on the ongoing concerns about the possible evolution of the COVID-19 pandemic and its economic ramifications which trigger adverse confidence effects worldwide, and a prolong the economic contraction. The narrative is

translated into a set of market and insurance specific shocks that generate a severe but plausible "double-hit" effect to the insurance industry.

For detailed information on the scenario and on the shocks, see the ESRB Adverse scenario for the EIOPA 2021 Stress Test, the Technical information and in the Technical specifications.

You may visit:
https://www.eiopa.europa.eu/sites/default/files/financial_stability/insurance_stress_test/insurance_stress_test_2021/2021-stress-test-adverse-scenario.pdf

https://www.eiopa.europa.eu/sites/default/files/financial_stability/insurance_stress_test/insurance_stress_test_2021/2021-stress-test-technical-specifications-v1.1.pdf

Approach

The 2021 Stress Test exercise assess the resilience of the European insurance industry by a capital and liquidity perspective:

- the capital assessment relies on the Solvency II framework;
- the liquidity assessment is based on the estimation of the sustainability of the liquidity position.

Participants are requested to estimate their position under two assumptions:

- Fixed balance sheet;
- Constrained balance sheet.

For detailed information on the approach see the Technical Specifications:
https://www.eiopa.europa.eu/sites/default/files/financial_stability/insurance_stress_test/insurance_stress_test_2021/2021-stress-test-technical-specifications-v1.1.pdf

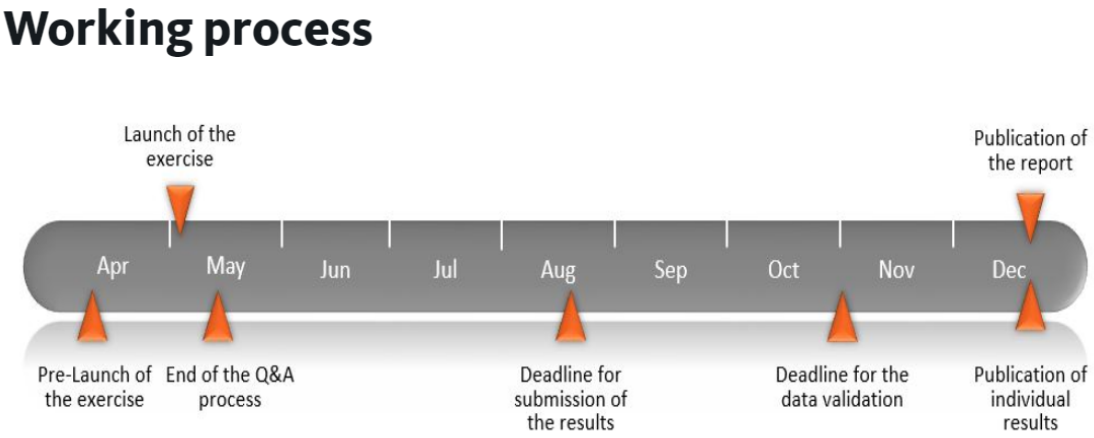
Scope

The 2021 exercise targets European (re)insurance groups. The selection of the participating entities is mainly based on size, EU wide market coverage, business lines conducted (life and non-life business) and number of represented jurisdictions.

The local market coverage was taken into account in a second stage.

The target sample defined in cooperation with the National Competent Authorities (NCAs) covers 75% of the EU-wide market based on total assets in the Solvency II.

The list of the undertakings in scope of the 2021 Stress Test exercise is reported in the Technical Specifications.



To read more:
https://www.eiopa.europa.eu/insurance-stress-test-2021_en

Number 3

Artificial Intelligence Governance Principles: Towards ethical and trustworthy artificial intelligence in the European Insurance sector.

A report from EIOPA´s Consultative Expert Group on Digital Ethics in insurance

Due to technological advances digitalised data and its use play an increasingly important role in our societies.

The amount of digital data doubles in short intervals, it is collected from different sources and formats and its manipulation gets more efficient. Data scientists invent novel ways of drawing better conclusions from the data.

Technology is finally making Artificial Intelligence (AI) into a relevant tool to improve our societies.

Insurance has been a heavy user of data from practically early days of its existence. The collection of data, even when available, has been expensive. Analysis of this data has been expensive too and often inaccurate.

Instead of an as exact as possible knowledge of insured persons and physical objects insurers have had to live with crude indicators of the risk inherent in each case.

The emergence of Big Data (BD) and AI are changing this, making it possible to have more exact knowledge and changing the ways insurers interact with policyholders.

Insurance has also through all of its existence dealt with ethical problems. Fair treatment of the insured pool and each policyholder has created problems that have been solved with varying degrees of success.

Developments with BD and AI are not creating new challenges in this area. Instead, they are offering possibilities to deal with some in a better way but also exacerbating other.

Current ethical issues in insurance are also acute only partly due to changes in BD/AI. Maybe even more often topical issues in this area result from changes in our societies, i.e., from changing thoughts on what a good life is and how individuals should be treated.

Ethics is about good life. There have been different efforts to formalise ethics, i.e., to create a framework to determine in an undisputed manner what is ethical and what is not. This has proved to be impossible. Therefore there cannot be an algorithmic way to integrate ethics into the use of data in a way that always reaches correct solutions.

This report approaches ethical issues in a more down-to-earth manner. Ethics is thought to mean approaches that are fair based on international and national recommendations, standards and treaties, and of course legislation. Our understanding is that this represents what most people would understand as ethical.

Insurance exists in many forms. One dividing line is between (mandatory) social insurance and private insurance. This report concentrates on private insurance. Possible issues on BD/AI in social insurance would need a separate analysis.

Ethical challenges in insurance result from separate interests of the main stakeholders of insurance activity. We can identify three key players:

- an individual seeking insurance cover or being insured,
- the pool of insured risks, and
- the insurer who manages the pool.

Usually the individual in this case is looking for suitable cover at a price that is as low as possible. The pool is a group of risks, independent enough that allows for risk sharing among the group utilising the Law of Large numbers or one of its softer forms. In the interest of the pool there should be certainty that none of its members is taking inappropriate advantage of the pool.

In many cases there are legal, contractual or informal ways of returning a certain part of the profit of the insurer to the pool and its insured even in situations where the insurer is a profit-making entity.

The requirements of insurability and the conflicting interests of these three stakeholders create situations with ethical dilemmas. In many cases this is related to the fair treatment of an individual when the interests of the pool and the insurer are taken into account. One can ask to what extent the legitimate interests of one of these players can be limited in order to honour the legitimate interests of the other two.

In our work we have looked at the challenges to fairness with the emergence of new technologies. Fairness is especially threatened with the treatment of individuals in more or less vulnerable situations. We have outlined tools in transparency and explainability to help identifying areas where fairness is

threatened. And we have suggestions on how the governance of the use of AI should be organised to safeguard sound use of AI.

The scope of our work was ambitious. Analysing how BD/AI influences insurance's many processes and interactions with policyholders was a significant challenge that we took eagerly knowing that compromises in the number of analysed cases would be required.

Some readers may wish that our report had covered specific forms of insurance in greater detail and provided more specific guidance for them.

We believe that, while not covering every possible case, our report provides the tools for individuals and organisations to reflect on the ethical challenges of BD/AI in insurance and apply BD/AI techniques in a trustworthy manner.

Should this require additional specialist knowledge, market participants (consumer associations, insurers and national supervisors) may want to work together in their respective markets to address those specific forms of insurance.

Figure 1 – Examples of AI use cases across the insurance value chain

Product design and development	Pricing and underwriting	Sales and distribution	Customer service	Loss Prevention	Claims management
▪ Historical customer and survey data analysis to inform new products ▪ Predictive modelling of disease development patterns ▪ Novel products, e.g. parametric and usage-based insurance	▪ Enhanced risk assessments combining traditional and new data sources (including IoT data) ▪ Price optimisation: micro-segment / personalised pricing based on non-risk individual behavioural data (e.g. to estimate price elasticity, lifetime value and propensity to churn) and market competition analysis	▪ Digital marketing techniques based on the dynamic analysis of online search behaviour ▪ Virtual Assistant and Chatbots that utilise Natural Language Processing (NLP) and insurance ontologies to support communication ▪ Proactive customer communication, nudging and cross-selling of related services ("next-best action") based on consumer data from Customer Relationship Management (CRM) systems	▪ Call centre sentiment analysis, route cause analysis, dynamic scripting and agent allocation ▪ Customer self-service through multiple channels using NLP, voice recognition, insurance ontology maps and chatbots ▪ Robotic Process Automation (RPA) including Optical Character Recognition (OCR) to extract information from documents (e.g. FNOL, email with questions complaints etc.) and route them to the correct department	▪ Provide diagnostic advice anc coaching based on AI analytics from health and automotive big data, e.g. suggest exercise and driving behaviour changes	▪ Enhanced fraud analytics: claims scoring, anomaly detection, social network analytics and behavioral modelling ▪ Loss reserving: use of AI to estimate the value losses, in particular for high-frequency claims ▪ AI image recognition to estimate repair costs in household property insurance, business premises and automotive ▪ Automated segmentation of claims by type and complexity and automated invoice verification and payment process

Source: EIOPA Consultative Expert Group on Digital Ethics in insurance

To read more:
https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa-ai-governance-principles-june-2021.pdf

Number 4

Opportunities and risks of central bank digital currencies

Burkhard Balz, Member of the Executive Board of the Deutsche Bundesbank, at the virtual European Payments Conference "Key Trends in the European Payments Landscape".

1 Introduction

Ladies and gentlemen,
Mr Maleki, Mr Bott,

Thank you for your warm welcome, and thank you for giving me the opportunity to deliver a keynote speech at today's conference.

The EURO football tournament kicked off recently, but things are rather different this year. There will be fewer gatherings in person and no "public viewings", as we say in Germany, with thousands of fans. Instead, I have already heard about public viewings taking place in the digital sphere, with fans using virtual conference software to get together and cheer on their favourite team.

Fortunately, the games themselves are taking place in real life – with a considerable number of fans in the stadium – and not virtually. The same still cannot be said for most meetings in the business world.

Therefore, I am also speaking to you in a virtual, digital format today.

However, digitalisation has also found its way into football, with teams using the likes of Big Data analytics to improve their performance. And we all know that money plays an important role in football business as well. So there is some common ground with the topic of our panel discussion and my keynote today: it is about rapid change, digitalisation and digital money, and central bank digital currencies in particular.

CBDCs are one of the most exciting developments facing central banks today – not just in Europe, but worldwide. Many questions need to be answered. Let me name just three of them:

What opportunities are associated with CBDC?

Is there a need for banknotes to go digital?

What features would cater to the demands of consumers and enterprises in both the financial and the industrial sector?

Maybe today's conference can shed some more light on the different components of these important questions.

Market experts in Europe and around the world are engaged in a lively debate about these questions, and several central banks are looking into the opportunities and risks associated with central bank digital currencies.

A survey among central banks by the Bank for International Settlements (BIS) shows a shift away from mainly analytical work on CBDC towards technical experimentation, with more than 60% of central banks reporting that they are running practical experiments.

However, central banks would be well-advised to be diligent and take their time. Because CBDC is a game changer – with huge opportunities, but also a number of risks.

Today, I would like to outline the issues I believe we need to tackle in order to create a safe, efficient and future-proof digital currency for Europe. Remember, just as in football, some well-executed tackles can win the game.

To lay the groundwork and provide some food for thought for today's discussion, let me briefly present three major trends in payments that are driving the debates on CBDC:

- The digitalisation of our economy,
- the declining use of cash, and
- emerging new forms of money.

2 Trends in payments

Our economy is becoming more and more digital, and the transformation is even gathering pace. E-commerce and all kinds of other online services are surging, and they are getting a further boost in the context of the COVID-19 pandemic. The Internet of Things is making machine-to-machine communications a reality, and it will likely result in a need for machine-to-machine payments.

The pace of digitalisation has probably never been faster than it is today. These developments are increasingly calling for a safe and efficient settlement asset including the appropriate infrastructure, in the sense of a digital currency that can be seamlessly integrated into almost any kind of business process.

At the same time, we are seeing a decline in the use of cash, even in Germany. The current pandemic has increased not just the use of cards, but of contactless payments and mobile payments in particular.

In a survey on payment behaviour in Germany conducted by the Bundesbank during the pandemic, we found that the share of cash for everyday transactions has fallen from 74% to 60% over the last three years.

Admittedly, it remains to be seen whether this tendency will persist in the post-coronavirus period. But what we are currently witnessing is a considerable change for a country that has been strongly accustomed to paying in cash.

A third trend is the emergence of new forms of digital means of payment. These can be privately issued means of payment, such as stablecoins, as well as CBDCs issued by foreign central banks.

For now, these alternative means of payment are still in the development or testing phase. However, given the speed at which the technology is developing, their widespread adoption might be closer than we think.

If these forms of money become widely used in the euro area as a medium of exchange or as a store of value, this could have severe implications: for the role of the euro, for the payment industry, and consequently also for financial stability in the euro area.

To read more: https://www.bis.org/review/r210617c.htm

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.

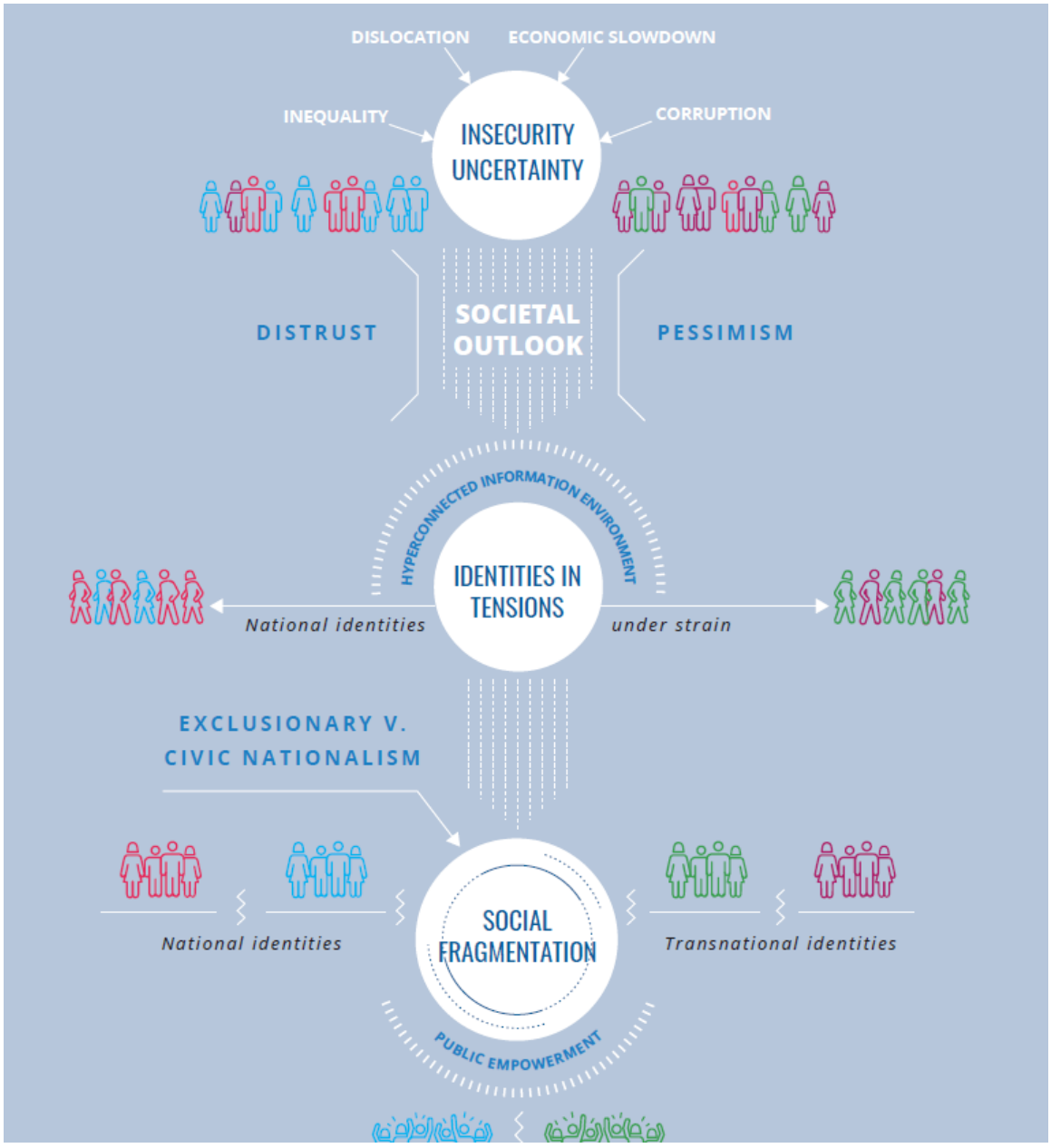
To read more: https://www.dni.gov/index.php/gt2040-home

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.

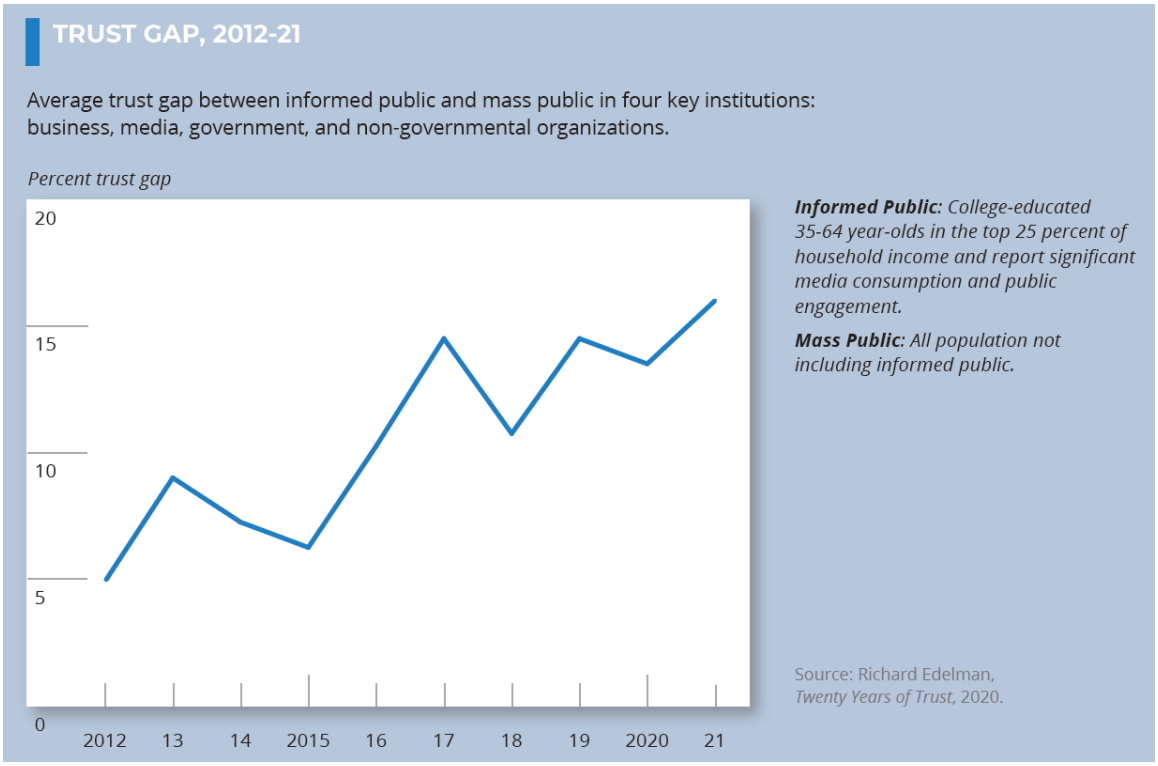
In a 2020 study of 16 developed countries by Edelman, the portion of the mass public trusting government since 2012 never exceeded 45 percent, and among Organization for Economic Cooperation and Development (OECD) economies, public trust in government fell in more than half of countries between 2006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

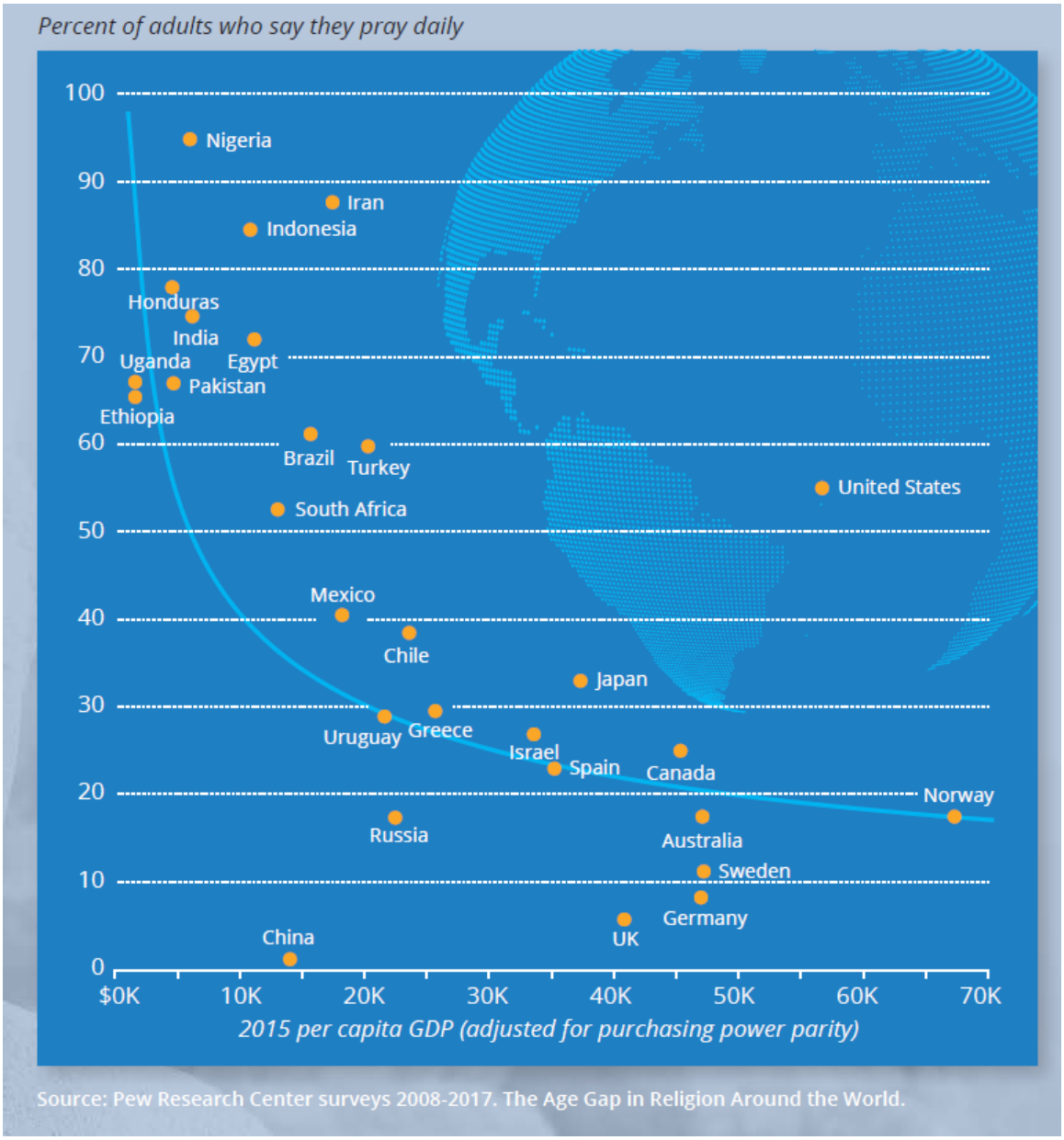
In less developed countries, corruption is undermining confidence in government, and people tend to trust informal institutions more than government where political power is concentrated among the wealthy elite.

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

Competition and collaboration: Understanding interacting epidemics can unlock better disease forecasts

By Andrey Lokhov

Epidemiological models took center stage throughout the COVID-19 pandemic, providing important information about the spread of the virus through communities and the world. But the spotlight on these models also illuminated their shortcomings. Early in the pandemic, several models were criticized for their lack of accuracy by either over or underestimating infection and death rates. This is understandable given that, early on, little data was available to feed these models. As the pandemic progressed and more data became available, the better they got.

But the new epidemiological models are still far from perfect. A recently developed algorithm aims to improve them by focusing on additional forces critical to spread but too often overlooked.

Until now, epidemiological models that forecast how viruses spread through populations have struggled to include concepts of collaboration among various diseases themselves that, once in the human body, increase the chance of a co-infection. For example, people living with HIV are 15 to 22 times more likely to get tuberculosis, and a person cannot contract hepatitis D unless they are already infected with hepatitis B.

To read more (URL given by Los Alamos national laboratory):
https://www.discovermagazine.com/technology/competition-and-collaboration-understanding-interacting-epidemics-can-unlock

Number 8

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 9

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.

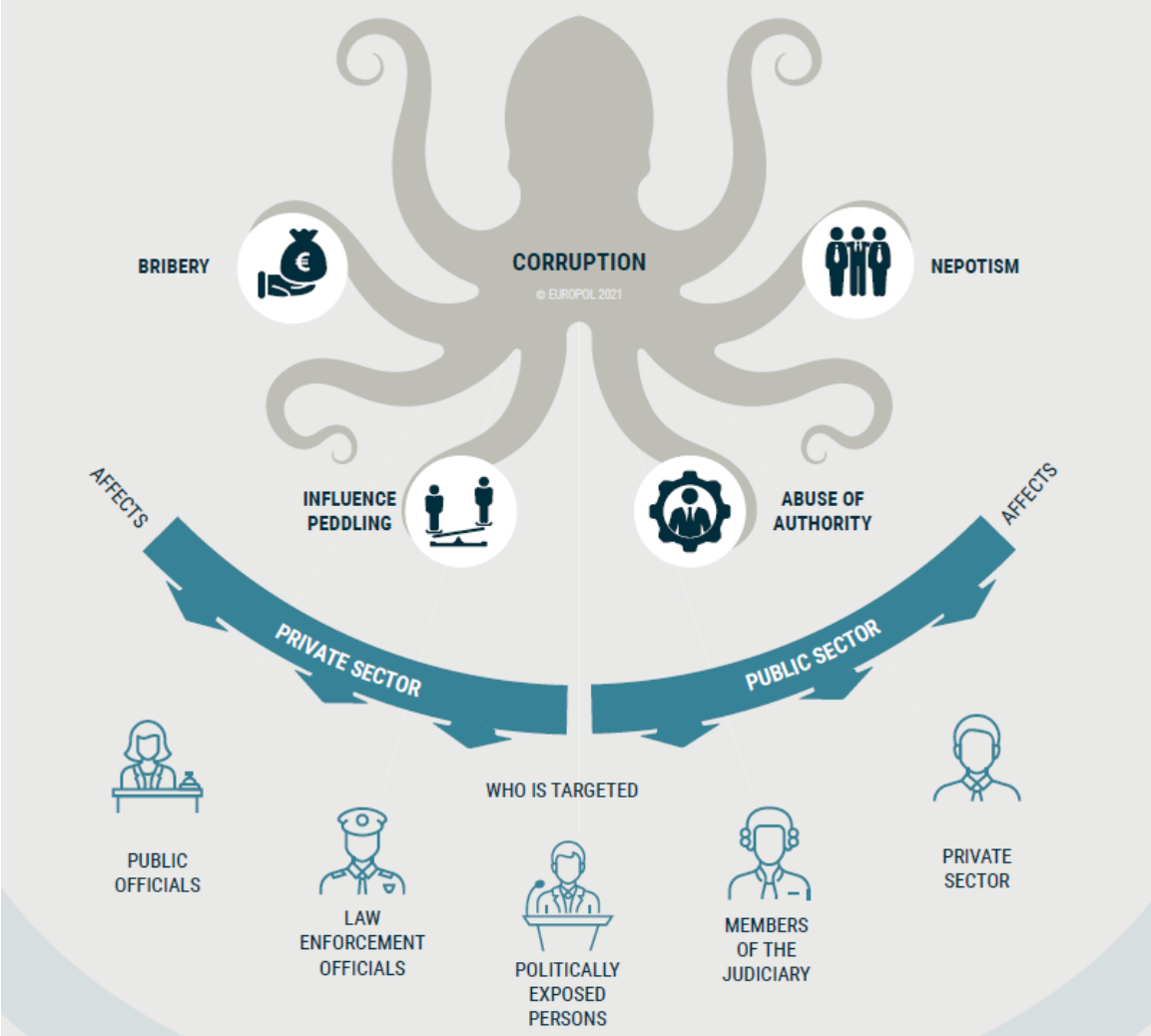
The use of technology is a key feature of serious and organised crime in 2021. Criminals exploit encrypted communications to network among each other, use social media and instant messaging services to reach a larger audience to advertise illegal goods or to spread disinformation. The online environment 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 10

Developing Morphogenic Electrochemical Interfaces

Advanced math modeling to enable new designs for persistent batteries, anti-corrosion coatings

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY

Persistent battery power and anti-corrosion coatings are key to sustaining military operations. Batteries power everything from tactical radios and handheld devices to unmanned systems.

Protective coatings shield flight surfaces, rotor blades, and ship hulls from corrosion caused by humidity, sand, and saltwater.

A challenge to creating more persistent batteries and coatings, however, is the inability to address microscopic irregularities that form at the interfaces of electrochemical materials.

DARPA today announced the Morphogenic Interfaces (MINT) program, which seeks to enhance the persistence of high-performance electrochemical systems by developing self-regulating interfaces that exploit detrimental local gradients to maintain optimal functionality over the planned operational life cycle.

The inspiration for pursuing novel, adaptive electrochemical interfaces comes from biology and the concept of morphogenesis, which explains the process of how cells and tissues take shape. A Proposers Day webinar for interested proposers is scheduled for July 9, 2021, from 11:00 a.m. to 3:00 p.m. EDT.

“Batteries and anti-corrosion coatings both rely on electrochemical reactions that take place at material interfaces from the atomic through millimeter scale,” said Vishnu Sundaresan, MINT program manager in DARPA’s Defense Sciences Office. “It’s at these microscopic interfaces that high energy density solid-state batteries and novel corrosion resistant coatings/alloys run into problems.

In solid-state batteries, as positively charged ions – lithium ions, for example – are deposited on the negative electrode during charging and then on the positive electrode during discharging, changes to the morphology of the interface leads to nanoscale voids at solid/solid ion transfer interfaces.

With each discharge/recharge cycle the number and size of voids at the interface increase rapidly and diminishes battery capacity until the battery

can no longer hold a charge. Solving the problem of voids at these interfaces is key to enabling practical solid-state batteries, which have high theoretical energy density and don't use organic liquid electrolytes that are common in lithium-ion batteries used widely today. Because solid-state batteries do not use liquid electrolytes, they're inherently safe from catastrophic fire up to 150 degrees Celsius."

Corrosion resistant coatings/alloys on ship hulls, power plants and critical aircraft surfaces undergo similar electrochemical reactions at solid/liquid and solid/vapor interfaces during cyclical loading, a process that happens anywhere from billions to trillions of times (cyclical loads) during the lifetime of the structure.

In aggressive corrosive environments, nanoscale pits that form at the material interface due to corrosion penetrate into the underlying metal and rapidly expand into larger cracks, weakening the hull, control surfaces, and engine components.

"MINT is focused on developing novel interface materials that can exploit local gradients to consistently form and reform at the interface," Sundaresan said. "The challenges in creating these interfaces and interface materials are due to our limited understanding of the evolution of 3D morphology and local gradients, which occur over five orders of lengthscale – starting with chemical interactions at the nanoscale and ultimately resulting in voids and pits at the micron scale. Current models for interfaces are one-dimensional and offer limited insights into the evolution of 3D morphology of the interface."

Morphogenesis was coined in the early 20th Century by D'Arcy Thompson, a Scottish naturalist mathematician, and the mathematical model for morphogenesis was first developed by Alan Turing. The concept of morphogenesis is so universal that it has been applied to pattern formation in almost any system – in geology, in the patterns on desert sands, floral patterns in plants, and even in 3D digital works of art.

"This approach can be naturally extended to electrochemical systems," Sundaresan said. "Through this program, I want to spur the scientific community to exploit the mathematical framework offered by morphogenesis models to understand the evolution of morphology in solid/solid, solid/liquid, and solid/vapor interfaces, and extend this understanding to build better solid-state batteries, corrosion-resistant coatings and alloys."

MINT development efforts are focused on two application-centric focus areas. The first is solid/solid charge transfer interfaces to enable solid-state

batteries with unprecedented combinations of energy density and cycle life. The second focus area addresses solid/liquid and solid/vapor interfaces for high- performance corrosion resistant coatings and alloys.

For more information about the MINT Proposers Day webinar, including registration details, visit: https://go.usa.gov/x68qB

A Broad Agency Announcement solicitation with full program details is expected to post on SAM.gov in the coming weeks.

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

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

- should not be relied on in the 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 an interpretative document;

- 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.

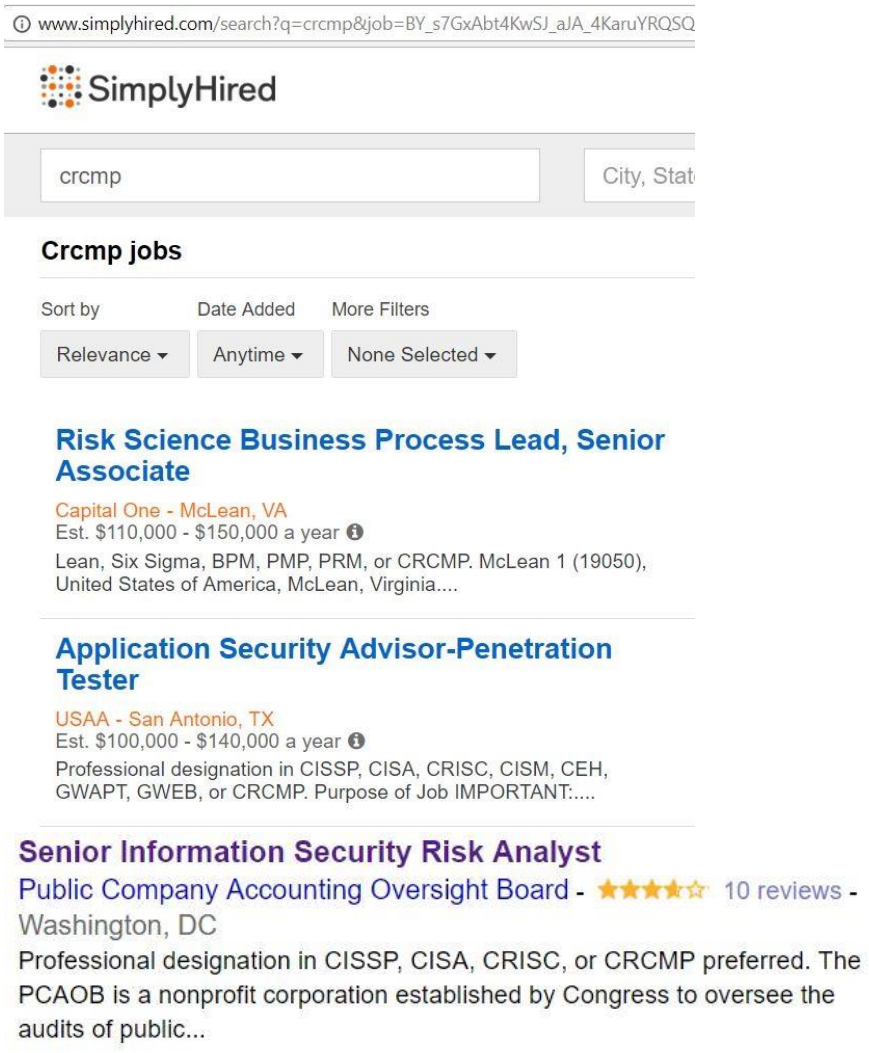
The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

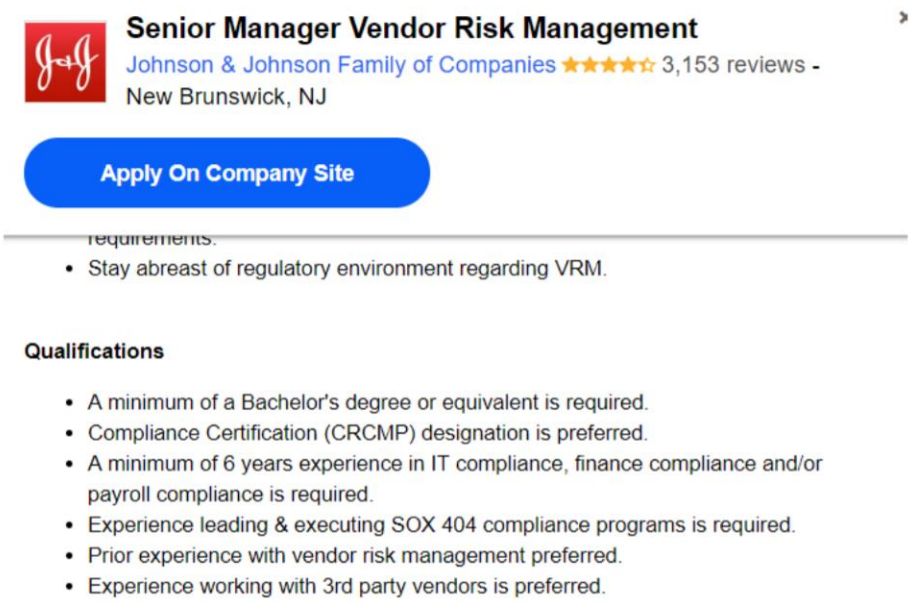
You can explore what we offer to our members:

1. *Membership* – Become a standard, premium or lifetime member.
You may visit:
https://www.risk-compliance-association.com/How_to_become_member.htm

2. *Weekly Updates* - Visit the *Reading Room* of the association at:
https://www.risk-compliance-association.com/Reading_Room.htm

3. *Training and Certification* – Become a Certified Risk and Compliance Management Professional (CRCMP), a Certified Information Systems Risk and Compliance Professional (CISRCP), a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, and / or a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I.





Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★☆ 3,153 reviews -
New Brunswick, NJ

Apply On Company Site

requirements.

- Stay abreast of regulatory environment regarding VRM.

Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

Companies and organizations like Accenture, American Express, USAA etc. consider the Certified Risk and Compliance Management Professional (CRCMP) program a preferred certificate. There are CRCMPs in 32 countries.

You can find more about the demand for CRCMPs at:
https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

For the Certified Information Systems Risk and Compliance Professional (CISRCP) distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:
https://www.risk-compliance-association.com/CRCMP_Re_I.htm

For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.