CIONET UK COMMUNITY PROGRAMME 2023

THE CYBERWAR

FACING OFF ROGUE NATIONS

Roger Camrass
CIONET UK

Discussion Documents

January 24

CIONET UK Community Programme 2023
The Cyber War:
Facing off Rogue Nations

This article is written by Roger Camrass, Director of Research for CIONET International. The content is based on the sixth UK Community Programme event of 2023, held on 22nd November 2023 at HMS Belfast, which was attended by 130 digital leaders.

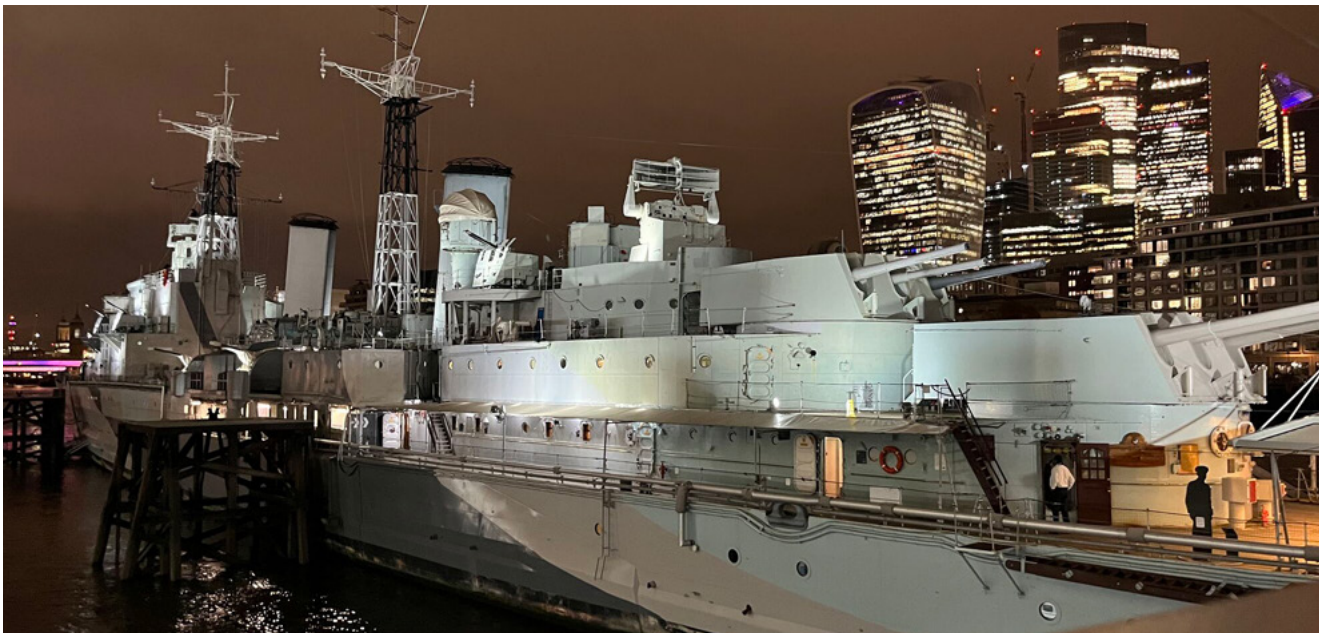
The context for the event

Cybersecurity continues to occupy a lead position in CIO priorities. Technological advances and changes to the political landscape mean the topic becomes increasingly important. Furthermore, rogue nations are likely to use artificial intelligence (AI) and quantum computing to disrupt commerce and public services in the future.

Cybersecurity, in short, remains a fast-moving target. But do our boards and employees comprehend the scale of the potential risks they face? In CIONET's final Community Programme event of 2023, we invited leading experts and practitioners to address key cyber issues, including:

- Who are the most likely sources of cyber activity – nation states or cyber criminals?
- How can IT organisations use data and predictive analytics to track cyber risks?
- What information does the board need to evaluate operational risks from cyber?
- How might emerging technologies, such as AI and quantum, change the cyber landscape?

The event followed our traditional format of a Master Class from a distinguished CIO leader, which was followed by a panel discussion of digital leaders and programme sponsors, including EY UK&I, CloudBees, Entelect, Infogain, Hitachi Vantara, and Thoughtworks. Here is a summary of the session.



Session One: A Master Class by Charlie Forte, Director General and CIO, Ministry of Defence

During his five-year tenure as CIO at the UK's Ministry of Defence (MoD), Charlie has helped transform the organisation into a software and data business. He drew an analogy with the event venue, HMS Belfast, which he described as a classic example of a military asset that can derive kinetic capabilities. Today, modern warfare is about software and data insights rather than just steel. This focus on data requires the integration of space, sea, land, and air capabilities. Cyber capability across these domains can mean the difference between winning and losing a battle.

1. **You say, 'you may not always be interested in geopolitics, but that geopolitics is interested in you.' What do you mean by this, and who should show the most interest in geopolitics?**

   So far, the UK has been well prepared and protected from major cyber disruptions. However, the political situation has changed dramatically during the past two years due to wars in Eastern Europe and the Middle East. The MoD has worked with GCHQ to evaluate the changing risk landscape and ensure we operate in an offensive rather than defensive manner.

   Charlie said our adversaries, which includes China, Iran, North Korea, and Russia, are investing vast sums in cyber warfare via state sponsorship and criminal gangs. The MoD says the UK is still operating below the war threshold, but this assessment could change. Organisations need to restate and refresh their understanding of where risks might emerge. The NCSC should be considered an essential partner in risk assessment endeavours. The CIO community should also listen to lectures on YouTube by MI5's Director General, Ken McCallum.

2. Could the global bifurcation between East and West influence who our enemies are in the future and the technology partnerships that we should pursue?

Charlie said we are experiencing a political bifurcation that will affect which technology partners we can work with and impact the long-term evolution of the global economy. He believes China's Belt and Road initiative, which is a global infrastructure development strategy, is providing economic leverage in certain regions, especially across the Global South. This strategy could place China in a more advantageous position in the future.

China is betting heavily on the success of its native technology partners, such as Huawei, whereas the West supports its digital pioneers, such as Nvidia and Microsoft. Charlie said Western organisations should think carefully about which strategic partners they use.

3. From your experiences at the MoD, who are the primary sources of cyber activity, and what areas are the highest defence priorities?

The MoD maintains a broad spectrum of capabilities to defend the UK from criminals and nation states. The organisation learned key lessons from the initial stages of the Russian invasion of Ukraine in 2021. For example, all digital capabilities were relocated during the first week of the war to ensure operational continuity. Big Tech played a lead role in this transition process. Despite heavy dependence on its legacy systems, Ukraine has adapted to the requirements of the conflict by renewing much of its software.

Some adversaries can have an advantage due to their ability to integrate systems rapidly. These adversaries, for example, do not need to conduct lengthy procurement processes. The MoD is upgrading its change programmes to exploit best practices in retail, banking and other commercial sectors.

4. How might CIOs best inform their boards about the cyber risks they face?

Charlie said the first challenge is to boost digital awareness within the board and across the management layers of the business. He believes digital awareness is a "team sport". At the MoD, he has introduced a world-leading digital learning programme for top executives. MI5 has helped design this programme.

5. You speak about the "grey zone" that exists below the threshold for war. Can you give examples of such grey-zone activities and their possible disruptive effects?

Charlie referred to China's use of TikTok as a means to educate young people about cyber. He said it is a national prerogative in China to ensure the population is conditioned to use cyber as a means of war. This approach contrasts sharply with the West, where TikTok is a social media platform that is used to exchange viral videos, such as dancing dogs.

When speaking about the grey zone, Charlie stressed the need for executives to monitor critical infrastructure, such as power stations and telecommunications networks. He said rogue states can implant viruses in these critical assets that can be activated at any time. Charlie said the safest approach is to assume these attacks will happen to your organisation and to take preventative measures now.

6. As many organisations, such as the MoD, become software-defined businesses, how do you ensure that cyberattacks are anticipated and prevented? Can AI help?

Executives must anticipate attacks at any moment, especially given the rapid pace of changes across the geopolitical landscape. Becoming a software and data-driven business exposes an organisation to a much higher risk of cyber disruption. The MoD makes a special effort to recruit the skilled individuals to address this problem. Given the potential vulnerability of national infrastructures, cyber skills are at a premium. The MoD gives talented cyber staff accelerated career prospects through its in-house training and development programme.

Session Two: Panel discussion

Four distinguished panellists were asked to comment on cybersecurity from the perspective of both their own organisations and their professional experiences:

- **Mark Adjei**, Director, Chief Information Security Office, Head of Cyber Security Risk Advisory & Governance – UBS
- **Rick Hemsley**, Cyber Security Leader – EY
- **Bridget Kenyon**, CISO – SSCL
- **Jim Gumbley**, Business Information Security Officer – Thoughtworks UK

1. What are the dangers to external supply chains, and can you give us some recent use cases?

Capita was attacked this year by the Black Basta ransomware group. The attack impacted Capita's clients, including the NHS, local councils, and government pension schemes. Capita is still recovering from the ransomware group's attack, which affected its Microsoft Office 365 software and accessed the personal data of staff working for the company and dozens of clients. This attack will likely cost Capita as much as £25 million.

The organisation of the criminal networks that operate in cyber space must be considered. These groups are federated businesses. For example, they have joined-up help desks that assist with payment.

2. How might AI affect cybersecurity, and how can such effects be mitigated?

There is no clarity yet as to how AI might assist in offensive and defensive cyberattacks. As Bridget Kenyon stated: "History is still to be written here." She believes AI will personalise cyberattacks, targeting specific individuals, including members of the board. Generative AI could act a force multiplier, making hackers and defenders more productive. Charlie Forte said the UK is an innovation leader that is likely to outmatch its adversaries. He also referred to efforts by Ukraine to track individual phones on the battlefield.

3. Are most cyber threats originating from internal or external actors? And what are the motivations of such actors?

Mark Adjei said he believes most attacks emanate from within the organisation, although it is unwise to neglect external forces. He said disgruntled employees are a significant threat, especially during merger and acquisitions (M&As). Mark said all CISOs should adopt preventative measures ahead of M&A activities.

4. What are the best tools and processes that can help your organisation to limit cyberattacks?

Attention must be given to staff at all levels, from the board down to software engineers. All staff members should receive education and training to ensure they understand their responsibilities. Mark suggested that organisations undertake an annual review of cyber policies and procedures to validate response planning.

Charlie said a collegiate culture is essential in efforts to avoid cyberattacks within an organisation, especially in a software-defined business. Cyber is a key theme within the MoD. He also said he believes the UK military is a global leader in cyber ethics.

5. Where does cyber fit into the modern CIO's ever-lengthening list of priorities?

Richard Hemsley said cyber remains in the top three CIO priorities, despite the rise of new challenges, such as generative AI. However, recent high-profile cyberattacks have helped to pique the interest of CEOs, who recognise that attacks can shut down operations for many months. He said many of the organisations that EY deals with expect their CISOs to present risk assessments to the boards every quarter. Charlie said the MoD uses this approach.

The recent migration of legacy systems onto public cloud platforms expands attack surfaces and increases cyber risks. CIOs are adopting security-by-design policies in their agile development environments, using methods such as DevSecOps.

6. Given interdependencies between enterprises and their many IT vendors, how can CIOs mitigate potential risks during contract and onboarding phases?

Jim Gumbley said standards, such as ISO 27001, provide a basis for vendor certification. All panellists stressed the growing vulnerability of organisations through external partnerships, especially when data is shared. Although audits can be helpful, the best approach is to develop trust and build collaborative relationships with key vendors. This approach can help to identify and resolve cyber concerns quickly.

Charlie said supply relationships often involve up to 10 parties. This kind of relationship means all supply chain members must be certificated, including via data protection agreements.

Concluding the event

Roger Camrass summarised the discussion by emphasising four best-practice lessons:

1. The sharing of cyber intelligence is critical in the UK. We have experienced organisations, such as the NCSC, that act as a hub for collaboration.

2. Organisations should review their cyber policies regularly, recognising that political and economic landscapes are changing rapidly.

3. The CEO and board should include cyber risk in their governance charter and receive regular assessments from the CISO.

4. Although we remain below the threshold for war, the preponderance of cyber incidents could escalate as countries, such as Iran and Russia, extend their military activities further into Europe and the US.

Roger Camrass
Researcher director

A pioneer of today's Internet as an ARPA research fellow at MIT in the seventies, Roger has spent over forty five years helping corporations harness the power of new technologies such as cloud, mobile communications, e-commerce, voice recognition and satellite. He was a partner at EY responsible for e-commerce during the dot.com boom. He is a graduate of Cambridge University and MIT, and a visiting professor at the University of Surrey.

See **rogercamrass.com**