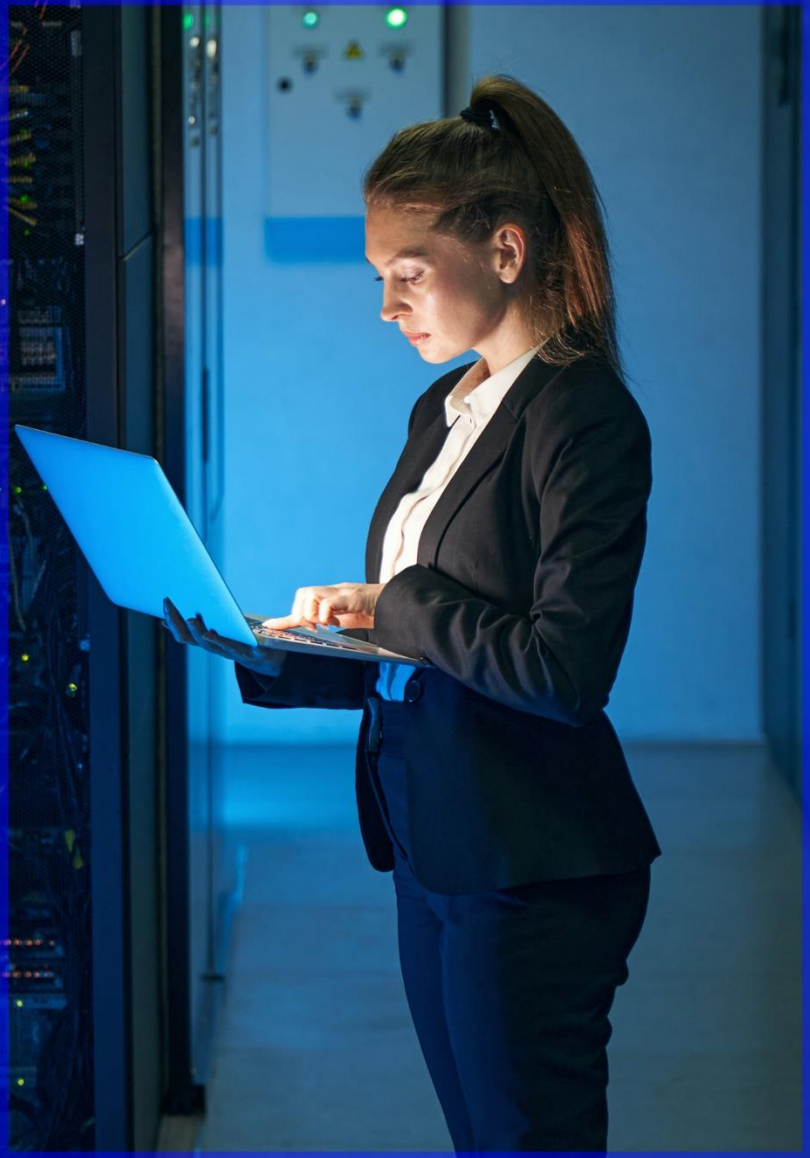
KPMG

The hostile limelight

The future of cyber in geopolitics



Introduction

A brave new world

The world has stepped into a new era of post-pandemic geopolitics. Some have argued that the pandemic signalled the end of an 80-year phase of globalisation, and brought existing undercurrents of geopolitical balkanisation up to the mainstream. In any case, the events of the last year have certainly marked the beginning of a complex period of political, economic and cultural upheaval, which we get a sense of every time we look at the news headlines.

We're witnessing an era of geopolitics characterised by the fragmentation and galvanisation of diplomatic relations and international treaties; turmoil in both domestic and international economies, trade and markets; protectionism over resources and skills, and resulting supply chain failures; highly active legal and regulatory regimes causing friction at the boundaries; the isolation of media and information technology networks; and the weakening and reshaping of cultural ties between regions of the world.

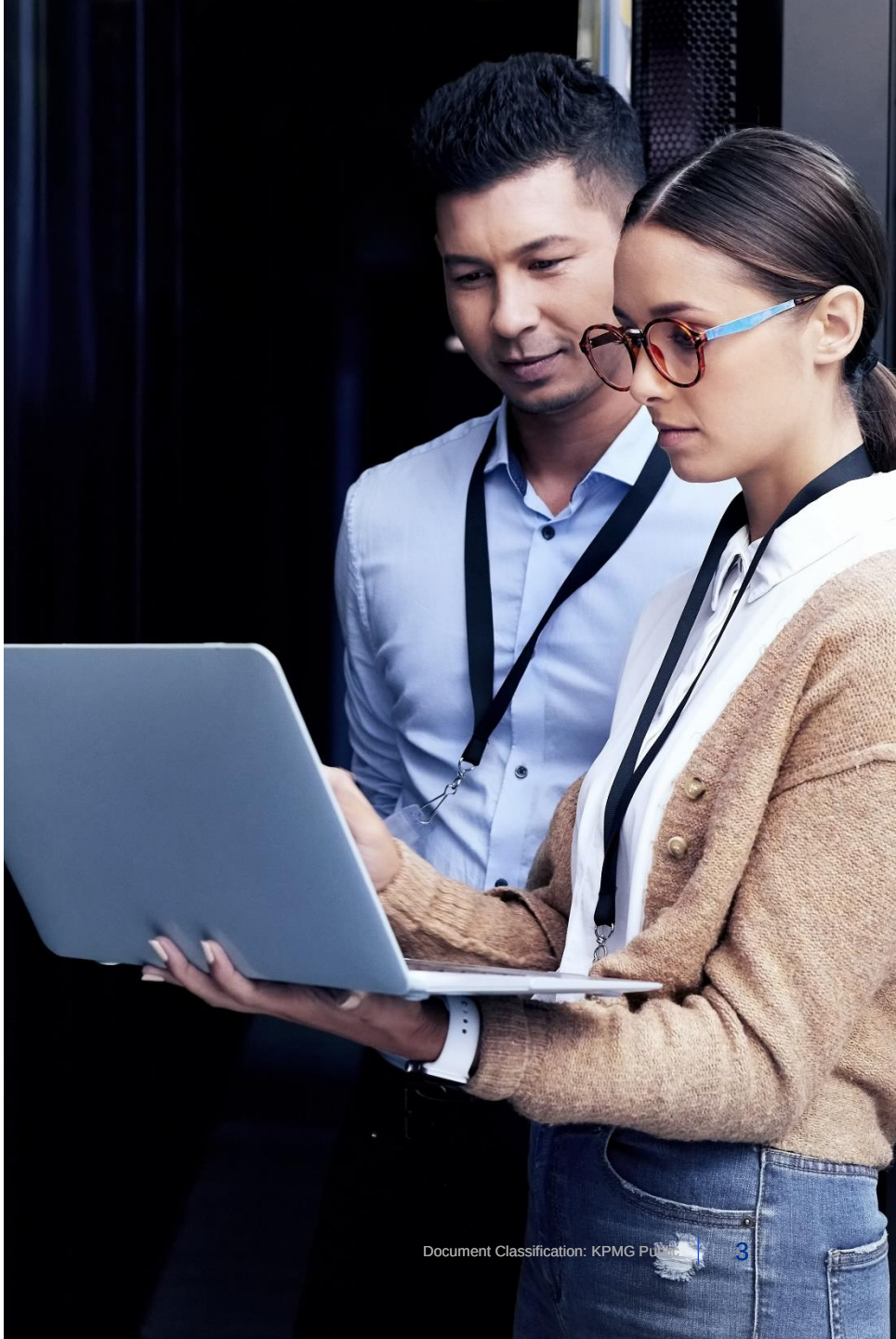
In this environment, the field of cyber security will play a dual role, in some cases exacerbating and in other cases providing solutions for the challenge we face in this period. The cyber profession, used to operating in the background, is now being thrust into an unfamiliar and hostile limelight.

Key themes and considerations

Organisations around the world need to factor the geopolitical risk to cyber security – and the cyber-driven elements of geopolitical risk – into their strategic decision making. We've put together some key considerations for organisations that can help weather the next few years of global affairs. These include:

- **Cyber in the conflict domain:** How organisations should adapt security and resilience processes to manage a geopolitically-driven threat landscape;
- **The evolving regulatory regime:** How organisations can prepare for a politically charged regulatory landscape powered by national security considerations, public trust and domestic politics; and
- **The media spotlight:** What organisations need to do to manage the risks associated with cyber in the media, and prepare their cyber teams for the spotlight.

Contents



Cyber in the conflict domain

Balkanisation typically breeds heightened military tensions and conflict between nation states and geopolitical blocs. As nation states build up both their offensive and defensive national cyber capabilities, we're seeing the first use cases of cyber in economic, military and environmental warfare, and parallel efforts at non-proliferation and international regulation. Despite efforts of international bodies, the balkanisation and weaponisation of cyber space has grown steadily through the 2010s, and there remains limited consensus among major geopolitical powers over how to govern nation state cyber activity. In the interim, the target and methodologies of threat actors will evolve, and organisations need to adapt:

Review resilience planning

The relative unpredictability and opacity-by-design of decisions made during conflicts mean that some scenarios may be difficult and impractical to plan for. Organisations should instead consider how to stress test the response of key elements of any scenario's resilience plan, including communications, personnel training, back-up and restoration processes, and decision-making capabilities under duress. Organisations should also consider the heightened risks of disruptive attacks around major national events and election days, and ensure resilience capabilities remain viable in the event that they are primary or collateral targets.

Update detection and response processes

Financial gain is often only a secondary objective of geopolitical cyber attacks; systemic disruption at politically strategic moments can often be the primary objective. Organisations should review their incident response (IR) plans and ensure they understand how to isolate and manage destructive malware and highly infectious, ecosystem-wide attacks. They should also maintain strong anomaly detection and network traffic analysis capabilities, in order to identify dormant malware or surveillance systems placed in advance of major attacks. Organisations should also conduct or support active threat hunting and intelligence gathering around known actors in order to bolster data sources for indicators of compromise (IoCs).

Cyber in the conflict domain (cont.)

Prepare for political hacktivism

As conflicts between adversarial nations and geopolitical blocs advance, organisations may face intense backlash for continuing to work in nations considered adversaries, or provide some services to hostile government agencies. Organisations who elect not to “self-sanction” (wind down operations in unfavourable jurisdictions) should review insider risk processes and harden security controls around easy targets like public-facing websites and media events, to protect against hacktivists that target companies for these perceived wrongdoings. Organisations should also consider new use cases and scenarios involving insider threats, especially risk relating to access and exfiltration of politically or legally sensitive data.

Collaborate across the ecosystem

Ecosystem-wide attacks targeting multiple organisations across multiple industries are likely to become more prevalent, mechanised by the growing vertical API integration of supply chains. Organisations should participate in industry-wide security collaborations and engage with external partners, suppliers, regulators and even competitors to share intelligence and security methodologies, as well as consider jointly testing IR plans. Capable organisations should consider their options on how to participate in active defence models in their industry, in the interest of ensuring that public and market confidence in their sector remains high.

Consider how to resource

As governments ramp up their investment in cyber, public sector salary budgets for key cyber capabilities, such as incident response, will grow to compete with the private sector. Cyber staff may be motivated to work by other considerations too, including a sense of civic duty to support national resilience efforts over private sector firms. Organisations should prepare to compete more directly with governments for top talent, and consider how to highlight their contributions to critical services and collective interests, in order to better position themselves for recruitment. They should also prioritise wellbeing initiatives to reduce the risk of burnout in their cyber teams, and improve retention of staff.

The evolving regulatory regime

Cyber security services have already attracted the attention of regulators. Historically, most regulation of enterprise cyber security and cyber services and professionals was motivated primarily by a concern for consumer safety and rights. Over the next few years, we're likely to see national security become the dominant lens through which cyber security regulations are defined. Organisations should prepare for the likelihood of:

Adapting to a fast-changing regulatory regimes

With national security posture as a backdrop, defence and intelligence communities may play a greater role in defining cyber security regulation in response to geopolitical events. Regulators are likely to make more sweeping changes, on shorter timescales and with less warning. Regulatory regimes may also harmonise or diverge with other jurisdictions depending on geopolitical factors, including to improve alliance relationships or the resilience of global supply chains for critical sectors. Organisations should conduct cyber regulatory horizon scanning with geopolitics in mind, and improve joint working between compliance and cyber security such that anticipated changes are appropriately implemented.

Legal barriers to cyber services and technology

Cyber security service providers may be prevented from providing some services, like vulnerability or threat intelligence and advanced detective tooling, to organisations in nations considered as adversaries. Conversely, other nations may prevent foreign service providers from working with domestic organisations on grounds of national security (e.g. anti-malware solutions, operational technology, or identity and access management services). Organisations should build out processes to vet cyber service providers under future laws or guidance, and stress test termination and contingency plans for key suppliers that may be affected.

The evolving regulatory regime (cont.)

Cyber security as part of critical national infrastructure

Some cyber security services may be scoped into critical national infrastructure regulation; these may include cyber managed services such as IAM, network infrastructure management, and IR services. Already, imminent regulations are bringing critical digital infrastructure into scope. As well as establishing appropriate vetting processes, organisations should factor in the heightened risk implications of some services: if a service provider is targeted to compromise one of their clients, other clients may become collateral damage.

Regulation of the cyber profession

Regulators are likely to impose skills and certification requirements on cyber professionals – already the case in other sectors – and impose tougher background screening requirements. The industry may also self-regulate. National security considerations may see restrictions imposed on some cyber security disciplines, limiting countries they are allowed to visit or live in. Organisations should proactively adopt regulatory and industry requirements, and keep up with best practice on regular background screening.

The media spotlight

Cyber security as an industry is already attracting press attention as cyber attacks grow in volume. As dependencies on the success of cyber security defences grow, the profession will be subject to even more media scrutiny that cyber staff are not typically trained to manage. Organisations need to be prepared to navigate the media and political environment.

Weaponising fear of cyber attacks

As exemplified in recent events, spreading information about large public data breaches or imminent cyber attacks, whether accurate or not, can lead citizens to limit their participation in economic, social and civic processes, or else trigger mass panic out of fear of disruptive attacks. Organisations likely to be the target of such campaigns should improve their logging, monitoring and forensic processes, so that they can confirm or deny reported attacks quickly and with relative certainty. They should also consider how to adapt their communications strategies to balance public safety and civic participation with their responsibility for transparency.

Propagandisation of cyber attacks

Major cyber attacks, especially those with a geopolitical lens, will attract significant media attention. Cyber will more commonly feature in political rhetoric in the approach to elections. Politicians may begin to directly refer to recent incidents, or else criticise organisations perceived to have not adequately protected consumer data or public services. Organisations should develop internal communications plans that set out the rules of engagement with media and journalists, and ensure that cyber professionals are sufficiently trained to handle media and political attention in concert with communications professionals. They should plan how to respond where cyber attacks on them are the subject of public backlash or political rhetoric.

The media spotlight (cont.)

Media scrutiny on third party cyber services

Cyber security service providers are likely to receive significant media attention following incidents where they are perceived to be involved or at fault. If a service provider is perceived to be at fault for an incident involving another organisation, their other clients may be pulled into the spotlight. Organisations should consider preventing the existence of cyber service contracts and alliance relationships to be made public. They should also establish and test information sharing protocols with major suppliers to manage how updates are shared following incidents, with both the media and with impacted stakeholders.

Public consciousness of cyber and privacy

Organisations should be prepared for a significantly heightened public consciousness of cyber security and privacy. National governments may begin major cyber awareness campaigns to prepare the public for major cyber attacks. Where governments are perceived to trespass on citizens' rights or freedoms, public campaigns and protests may gain momentum. Organisations should screen for the reputational risks of providing some government contracts both domestically and internationally, and involve CISOs, DPOs and technology ethics advisors in decision making processes around some commercial contracts and services. They should also more strongly factor in reputational risk when considering the impact of cyber attacks.

Navigating the new terrain

Cyber is a profession used to operating away from the spotlight. In the current geopolitical environment, this is no longer an option.

Organisations will need to take steps to manage the new geopolitical threat landscape, keep up with the evolving regulatory regime, and manage heightened media and political scrutiny. These challenges are rapidly becoming a part of our daily discussions with clients, as they grapple with the long term picture.

Please get in touch to join the conversation, and let us know how we can help.

Authors and Contributors

Ravi Jayanti

Manager – Cyber
KPMG in the UK
ravi.jayanti@kpmg.co.uk

Martin Tyley

Partner – Cyber
KPMG in the UK
martin.tyley@kpmg.co.uk

Tim Fletcher

Director – Cyber
KPMG in the UK
tim.fletcher@kpmg.co.uk

Ali Abedi

Senior Manager – Cyber
KPMG in the UK
ali.abedi@kpmg.co.uk

David Ferbrache

Global Head of Cyber Futures
KPMG International
David.Ferbrache@kpmg.co.uk

Contact us

Del Heppenstall

Partner - Head of Cyber UK
KPMG in the UK
del.heppenstall@kpmg.co.uk

Julia Spain

Partner - Cyber Strategy & Risk Lead
KPMG in the UK
Julia.Spain@kpmg.co.uk

Richard Krishnan

Partner - IGH
Cyber
KPMG in the UK
richard.krishnan@kpmg.co.uk

Matthew Martindale

Partner – FS
Cyber
KPMG in the UK
matthew.martindale@kpmg.co.uk

Serdar Cabuk

Partner - Sectors
Cyber
KPMG in the UK
serdar.cabuk@kpmg.co.uk

kpmg.com/uk

Document Classification: KPMG Public

CREATE: CRT146549A