ATKINS

Member of the SNC-Lavalin Group

The future challenges of Defence cyber

Authors

Phil Davies
Defence Cyber Lead, Atkins

Dr Richard Piggin
Principal Operational Technology
Cyber Security Consultant, Atkins

Introduction

Technology is evolving faster than ever before, connecting our day-to-day lives and providing opportunities for business and social interaction. Yet this ever-increasing interconnectivity also provides opportunities of attack from those who want to create disruption and cause harm. Cyber attack is a hot topic in the news as governments, companies and citizens find their data being stolen and their networks compromised.

At the same time we are witnessing rapid urbanisation around the world. By 2035, the majority of the world's population will be living in urban environments, with the global population predicted to rise from 7.2 billion in 2015 to between 8.1 and 9.4 billion. Africa and Asia are urbanising most rapidly and by 2035 Africa will be the fastest urbanising region in the world. Megacities, with populations of over 10 million people will continue to be created. It is predicted that there will be over 40 by 2035.

These huge shifts in our world will create a very different living and working environment for us all, and particularly for Defence. The need for military operations to support stabilisation in these emerging megacities when conflict happens, coupled with a growing trend for cyber attacks against the systems that support these cities, sitting behind the Critical National Infrastructure (CNI) that provides water, power and even health services, mean that we are looking at operating in a very different world to the one we know today.

Defence and cyber

The Defence sector, and the UK Ministry of Defence (MOD) in particular, has long been alive to the opportunities and risks of operating in cyber space. Featuring in the Strategic Defence and Security Review in 2015 and Ministerial announcements since, cyber is regularly discussed and rarely out of Defence news publications.

In response to the evolving threat of cyber attack, the MOD has formed the Joint Cyber Group, Front Line Commands have created Cyber Protection Teams (CPTs) and industry has been engaged to conduct Cyber Vulnerability Investigations of Defence platforms and systems.

More broadly, cyber is being merged with wider electromagnetic activities with the announcement of plans to form Cyber and Electro-Magnetic Activity, or CEMA, regiments in the Army. This demonstrates the MOD's desire to weave cyber into the fabric of defence.

These emerging UK Cyber Protection Teams are focused on existing, military-owned or operated networks and can conduct:

- Incident response - to react to cyber-intrusions and recover system capability
- Asset and vulnerability discovery – to create a baseline map of assets which need to be protected to conduct vulnerability assessments
- Behavioural monitoring and log analysis - to monitor and detect suspicious activity on the network
- Intrusion detection and packet capture - to protect the network from malicious activity, whilst capturing packet data for future investigations
- Digital forensics - to analyse malware and conduct incident investigations
- Cyber Threat Intelligence - to research, understand and report on the prevailing threat in cyberspace.

Cyber and Electro-Magnetic Activities are already defined in Defence Instructions and Notices and a new CEMA Doctrine is emerging in the UK, with a second edition recently being published by the United States Army.

However, to really understand the challenges we are likely to face in the future, we need to step away from the issues of today, and look forward to a period when many of the platforms, systems and capabilities currently in service will have been retired.

To put us in that future epoch we must first examine the future operating environment, for which the Defence Concepts and Doctrine Centre (DCDC) has already provided a strategic context and characterised to inform security policy makers.

The future operating environment

And General (Ret'd) Sir Richard Barrons succinctly summed up the future operating environment as:

"A wide range of state and non-state actors will exist, able to deploy and employ effective forces; confrontation will be common and conflicts less predictable. Micro global trends will produce seeds of new confrontation, played out in large urbanised areas where power, wealth and force reside."

So, while the future is hard to predict, everyone is clear that the amalgamation of the following will create a combustible mix:

- megacities that will become the political and economic centres of countries,
- advances in technology creating greater connectivity,
- and the potential for unpredictable conflict

The MOD's Future Operating Environment 2035 report identified the following key themes of the future operating environment:

Globalisation and interconnectivity

Shifts in the balance of power

Demography

Urbanisation

Climate change

Resource scarcity

Technology

Corruption and criminality

Relationships with the state

In this new environment, achieving effective cyber resilience will not just be about defending military systems and networks, or finding more servicemen in each of the Front Line Commands to form more military CPTs. Military forces operating overseas will find themselves in urban environments with less time to prepare, and even shorter time to deliver effective responses on the ground and hostile actors will be able to exploit and disrupt not just locally but from a distance. They will be reliant on extended lines of communications from the UK and supply chains reaching into the industrial base. Therefore, the challenges of cyber security in the future will be very different to today. As a result, it will inevitably also require the cyber protection of the local Critical National Infrastructure.

What is Critical National Infrastructure?

Critical National Infrastructure (CNI), is infrastructure deemed essential by nation states. In the UK, the Centre for Protection of the National Infrastructure (CPNI), defines CNI as:

"Those critical elements of national infrastructure (facilities, systems, sites, property, information, people, networks and processes), the loss or compromise of which would result in major detrimental impact on the availability, delivery or integrity of essential services, leading to severe economic or social consequences or to loss of life."

The UK CNI also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public, such as civil nuclear and chemical sites.

This CNI is operated by Operational Technology (OT) which are the systems that combine sensors, actuators and network connectivity that have a potential physical impact on our infrastructure. This includes Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems, known as ICS.

What's changed?

So is this threat to local critical infrastructure really new? Brigadier (Ret'd) Phil Davies' own experiences in helping establish the International Security Assistance Force (ISAF) in 2001 suggest not. Following Western intervention, the Taliban was removed from power. At a time of uncertainty and danger, the population in Kabul increased as some of those from nearby provinces sought refuge. Electric power was already unreliable and was straining to meet increased demand. The lights were literally dimming and it became an issue for ISAF as crime increased and 'blood-letting' was apparent as long-held scores were settled. ISAF was overseeing a breakdown in security, not improving it. Its credibility was called into question, exploited by those wanting a return to pre-intervention status quo and undermining efforts to secure wider contributions for the international coalition.

Military forces under UK command were on the ground, and able to engage face-to-face with civil ministries who had two key questions: were the hydro-electric dams outside the city intact; and, if so, could repairs be made to provide the capital electric power. Reconnaissance parties were deployed to the dams, surveys of power distribution systems (which also carried rudimentary communications) were completed by Royal Engineers and communications specialists from the Royal Signals designed, procured, installed and trained local users in HF and VHF communications systems. The water flowed, the voltage increased and they ultimately turned up the lights some months later.

This is not a one-off event. Similar issues arose in Iraq when utilities were unreliable and even basic sanitation could not be provided to a frustrated population. So whilst not a military objective from the outset, deployed military forces had the ability to react as they were on the ground, but had no mandate and limited expertise, yet the delivery of these essential services became critical.

The threat against Operational Technology

Until recently, the prospect of a cyber attack impacting Critical National Infrastructure and the operational technology that sits behind it to delivery public services was largely theoretical. However, it became a reality on 23 December 2015, when Ukrainian media reported that a cyber attack had left half the homes and 1.4 million people in the Ivano-Frankivsk region without electricity.

A cyber attack had left half the homes and 1.4 million people in Ukraine without electricity.

Although services were restored within a few hours, it was the extent of the attack that was cause for concern. Further investigation revealed that the incident was not isolated and that multiple electricity companies had been affected simultaneously. Similar malware had even been found in IT networks at Kiev's Boryspil Airport, including a network used for air traffic control. Ukraine blamed Russia for the incidents.

Later, the presence of Black Energy 3 malware was confirmed, as well as the fact that the power outages were caused by remote cyber intrusions at three regional electric power distribution companies. Three other organisations, some from other critical infrastructure sectors, experienced intrusions but were thankfully unaffected. The cyber attack was synchronised and coordinated, following extensive reconnaissance of the victim networks. Although this represents the first confirmed attack against the electric power grid, there has been much widely reported reconnaissance, such as the Havex malware of 2013 and 2014.

So what does this mean for the deploying military force in the future? Atkins undertook some funded innovation research through the Centre for Defence Enterprise (now replaced by the Defence and Security Accelerator) under Defence Science and Technology Laboratories (Dstl) to find out. While the research report itself is currently under review, some of the trends and evidence gathered to support this work is of particular interest.

Atkins' analysis of infrastructure trends, drawing from those who are designing and advising on the creation of the megacities of the future, has identified some key themes for Operational Technology in Critical National Infrastructure including:

- Increasing digitisation of Operational Technology, machine-to-machine communications via enterprise networks that can unwittingly create unfettered access to the Internet
- Ubiquitous network connectivity that exploits Software Defined and Time-sensitive Networks, mobility and cloud technologies
- Increased use of data analytics. For example in the Water industry where sensors for leak monitoring are leading equipment manufacturers to develop software that optimises performance and therefore increases profitability
- Developments in telecommunication will introduce new services, used by asset owners to operate infrastructure
- Utilisation of common communications architectures, replacing proprietary control protocols with open network technologies, which were later moved to IP networks
- Potential to 'leapfrog' legacy technologies and adopt the latest available technologies, e.g. wireless.

This means that increasingly and definitely by 2035, technological change means that hostile actors can influence from a distance, not just by coercing the local population or attacking facilities and they will not need to resort to kinetic attack to deny use of or degrade Critical National Infrastructure, making military operations on the ground far more challenging.

So what is driving these conditions?

The fourth industrial revolution

'Industry 4.0' or the fourth industrial revolution, is a global hot topic for those philosophising about the benefits to mankind from the enormous changes predicted. It was the theme of a World Economic Forum in Davos in 2016. Reports highlighted the changes in how people live and work through the combination and adaptation of rapidly evolving information technologies, including data, processing, connectivity, artificial intelligence, robotics, autonomous systems, space, bio-sciences and nano-technology.

Atkins' Infrastructure design and advisory experience suggests the following trends that will have greatest impact on a military deployment:

- Convergence of Information Technology (IT) and Operational Technology (OT)
- Rapid evolution and connectivity of the Internet of Things (IoT)
- Operational Technology development lag
- Legacy and modern systems integration
- Emerging technologies in support of infrastructure and/or embedded within
- Developments in data analytics, artificial intelligence and machine learning will provide opportunities and threats.

Convergence and the interconnectivity of systems will offer undeniable efficiencies. However, Atkins' Safety and Security consultant, Dr Richard Piggin is a cyber security advisor to UK CNI providers, to draw conclusions on the reliance on networking and critical integration of safety and security strategies in future. He explains:

"Several challenges arise in convergence and implementation of networked safety systems used in hazardous applications. Not least, the separation of the safety engineering and security disciplines. Where safety and security risks intersect, lies cyber induced safety hazards. Security mitigations need to be assessed to ensure they do not introduce new safety risks.

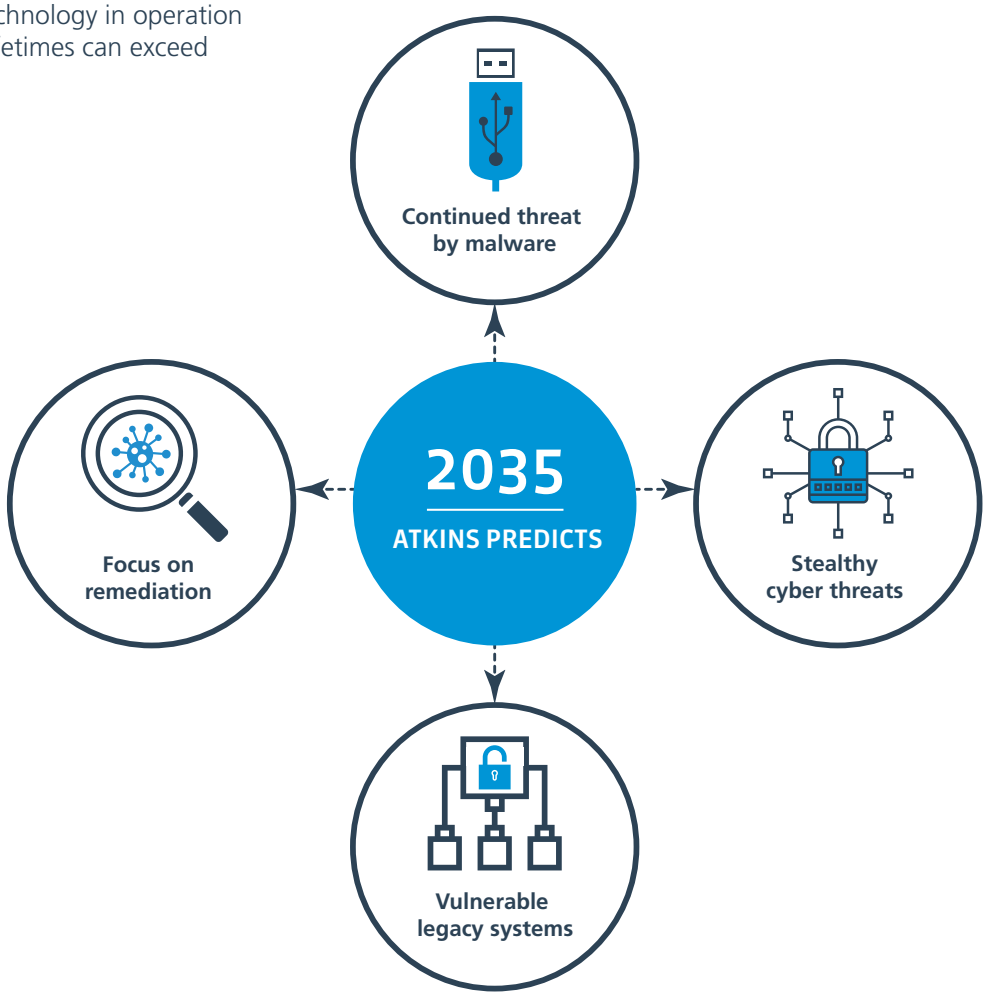
Potential tensions are illustrated with the rigorous approach to safety engineering versus the very dynamic and subjective nature of cyber security. An intelligent adversary could consider a chain unsafe events and use those as goal-based outcomes. Thus, undermining safety protection measures or intentionally triggering known safety functions, affecting processes, with the intent to deny asset use."

Future cyber security challenges

So how will the threat evolve over the next 20 years? By 2035 we predict that there will likely be a wider set of threat actors in cyber space.

- In general, computers, networks and information systems will continue to be compromised by malicious software, or by corrupting the supply chain.
- It may not be immediately apparent that disruption to systems is malicious in nature, and not just a result of component failure.
- From a Critical National Infrastructure perspective, by 2035 cities and infrastructure will be dependent upon ubiquitous connectivity for sensing and control, distributed intelligence, and automation. Secure engineering design of these cyber physical systems (used in infrastructure), must then be the norm. However, legacy infrastructure technology in operation now, will remain in use as their lifetimes can exceed 20-30 years.
- Asset owners, even those demonstrating high cyber security maturity, will be constrained by their business models and the economics of cyber security. Their cyber security approaches will be highly unlikely to be able to prevent high-end nation state intrusions, but instead focus upon early detection and restoration of operations/services.

This is already the approach of mature CNI cyber security strategies, where the focus considers the capability and intent of specific threat actors, and the most appropriate resilience outcomes. Cyber resilience – a term which Atkins uses to describe the ability of an organisation to understand the cyber threats it is facing, to inform known risks, to put in place proportionate protection, and to recover quickly from attack – will likely be just as relevant in the future as it is now.



Challenges for Defence

Increasing urbanisation and the growth of megacities of scale and complexity will be challenging to host nations, let alone international military forces. Communications and connectivity are such that tensions will quickly capture international attention and events will be played out in front of a global audience.

Nation states are already developing military cyber capability, with widely reported incidents of cyber intrusions. According to the Institute of Strategic Studies, who examined the evolution of the cyber domain, by 2035 it is expected that cyber capabilities will be fully integrated into military operational processes, including targeting.

Adversaries with global state sponsors will be able to threaten host nation owned CNI; they will be adaptive and able to develop malicious effects drawing on supporters and sympathisers connected globally. Some of these could result in physical damage, not just the interruption of infrastructure upon which military operations depend.

So what does this mean for military commanders? Recent work in Atkins has focused on specific areas of a military component as part of a wider, pan-government response to an emerging crisis in an overseas megacity. It is not a scenario in the more demanding spectrum of operations, but it concludes that military commanders and planners must identify the Mission Critical Infrastructure upon which their operations depend. This includes, but is not limited to, those elements of a host nation's Critical National Infrastructure on which mission success is reliant:

Doing so will require an understanding of a country's cyber maturity, the assets on which the military force depends, as well as those required by partners across government, allies and non-government organisations that are operating in that country or megacity. Mission Critical Infrastructure will change over time, as the campaign matures.

The Combined (from a number of nations) and Joint (from all armed services) force will be supported by national and international agencies in a full-spectrum plan; a whole-force approach. It will be expected to protect and sustain itself against an array of capability in a complex urban environment, probably at the end of lengthy lines of communications passing through several neutral nations. Military command and control will likely be primarily delivered by reach-back to resilient, connected allied headquarters, significantly reducing the number of staff officers supporting levels of command. There will not be spare military personnel who could be re-employed to meet emerging or unexpected needs.

Stabilisation forces seeking to influence events overseas will be dependent on the host nation's infrastructure. Moreover, citizens will expect working utilities as part of the overall improvement to security and stabilisation provided by foreign forces.

Conclusions

The evolution of the cyber threat and the future operating environment pose real challenges for Defence cyber. Resiliency of Mission Critical Infrastructure is an enduring task and capability will be necessary throughout all phases of a military campaign. It will require an understanding of the host nation's Critical National Infrastructure before deployment. This is not something that can be done at short notice and by military intelligence staff alone.

The success of an intervention will be dependent on protecting that Mission Critical Infrastructure. Its resilience – both in protection and ability to quickly recover after a cyber attack – is essential to support the military component and ensure provision of the basics of human life in megacities, including power, food and water.

The fusion of legacy and future infrastructure technology will bring with it a new set of cyber vulnerabilities. It is unlikely that by 2035 there will be the global cyber security frameworks, standards, technology and processes that can protect these inherent vulnerabilities.

This is not just a role for deployed military Cyber Protection Teams. An overall deployed military force will require greater understanding of the operating environment, including Operational Technology on which Mission Critical Infrastructure depends. Cyber Protection of Mission Critical Infrastructure must now be integrated into the campaign plan and not be left as a niche activity for specialists on the fringe. Emerging CEMA doctrine presents the opportunity to address these broader vulnerabilities and not just focus on that of military systems. It requires the integration of cyberspace activities, i.e. CEMA, into the military (and potentially political) estimate, force generation (with allies), planning and deployment through air and sea points of disembarkation. Enhanced cyber protection may also require deception measures if surprise is sought and freedom of manoeuvre is deemed to be essential. Passage through neutral ports or open skies and seas may require its own cyber protection to counter remote disruption from hostile adversaries.

Existing military-only Cyber Protection Teams do not have the full skill sets to face these challenges. They need to engage specialist knowledge through a combination of Reserves (Reserve Squadrons in Army CEMA regiments, and other Specialist Reserve units with appropriate engineering and cyber expertise for example), contextual knowledge from those in air or maritime domains, and contractors either through reach-back to specialists in industry or in-theatre. Control Systems security knowledge, including industrial software and protocols, and engineering expertise is presently scarce and lies within UK industry. These skills, and people, are in high demand and their knowledge will be required by those seeking to understand, and mitigate risks to Mission Critical Infrastructure. Partnerships between the military and such organisations and wider industry will provide the necessary technical expertise.

The world as we know it will continue to evolve and the impacts of urbanisation and technological change will endure. Meeting the challenges and protecting against the risks of this future operating environment will remain. Therefore, to achieve mission success, keep civilians safe and megacities functioning, the reality is that a range of skills and experience from a wide array of parties will become ever more essential.

Authors

Phil Davies
Defence Cyber Lead

Phil Davies retired from the Army in 2012 after 28 years' service. He spent much of his career overseeing the delivery of the secure communications, IT and physical headquarters that enabled deployed military commanders to execute command at both the tactical and operational levels. Over the last five years he has worked in industry, initially delivering secure networks and gateways to help Government customers counter cyber security threats. Latterly operating as a consultant with experience in the Middle East in Joint Logistics, he is now working with design, engineering and project management consultancy Atkins to further develop their cyber resilience and security capabilities across the Defence and Critical National Infrastructure markets.

Dr Richard Piggin
Principal Operational Technology Cyber Security Consultant

Richard is a security consultant at Atkins. He has an Engineering Doctorate in industrial networking from the University of Warwick and has since focused on networking, technology evangelism, international standards, safety and security. He is a member of the IEC standards working group bridging safety and security. Richard also chairs the IET Cyber Security Technical Professional Network, a thriving community that enjoys membership from across all of the Institution's sectors. At Atkins, Richard is working with clients to make their Operational Technology resilient against current and emerging threats.

References

[1] MOD Strategic Trends Programme, Future Operating Environment 2035. As part of the strategic trends programme, the Defence Concepts and Doctrine Centre (DCDC) looked to 'describe the characteristics of the 2015 operating environment to provide evidence-based insights that can inform future capability development'.

ATKINS

Member of the SNC-Lavalin Group

www.atkinsglobal.com/cyber

defencecommunication@atkinsglobal.com