WALTER SCOTT

BNY MELLON | INVESTMENT MANAGEMENT

The RESEARCH JOURNAL

BUILDING **RESILIENCE**

Extract from The Research Journal, Issue 14.

Russia, China and various shadowy groups hostile to the West have pipelines, oil and gas platforms and subsea internet cables in their sights. Senior Chatham House Fellow Armida van Rij assesses the risks

Consider the challenges a global company would face if it were suddenly impossible to contact colleagues and clients on the other side of the world. Imagine financial transactions consistently being declined. Energy supplies being so scarce that populations cannot afford the sky-rocketing costs. Such scenarios would not only cause disruption to global markets but would also risk social unrest. These scenarios become likely realities if critical infrastructure such as pipelines, oil and gas platforms, and subsea internet cables are compromised.

And yet the West's adversaries have been building up their arsenal of hybrid warfare tactics, combining military and non-military attacks to do exactly this. All without firing a single shot into NATO territory. Many such attacks are in the so-called 'grey zone': attacks below the threshold of war. Russia,

ARMIDA VAN RIJ
Armida van Rij is a Senior Research Fellow at Chatham House and heads its Europe Programme. She advises governments on a range of foreign, security and defence policy issues. Previously she was a Research Fellow at The Policy Institute, King's College London.

China and non-state actors have used such tactics for espionage purposes, to cause disruption to communications and energy supplies, and to fray societal cohesion.[1]

"While the West is currently rightly focused on conventional warfare, it risks overlearning the lessons from Russia's invasion of Ukraine"

While hostile actors cannot launch a full-scale attack on a NATO country without prompting a response, they have successfully used grey zone warfare instead. These attacks are more difficult to attribute and respond to and are therefore a popular weapon for adversaries who seek to disrupt societies without triggering a fully-fledged response. Attacks of this kind are not carried out only by states – there has also been a proliferation of state-affiliated groups that perpetrate grey zone attacks, as well as continued attacks by non-state armed groups.[2]

THE RISKS TO OFFSHORE AND SUBSEA INFRASTRUCTURE

While the West is currently rightly focused on conventional warfare, it risks overlearning the lessons from Russia's invasion of Ukraine. For Russia in particular, deploying grey zone warfare against the West has become more important as it seeks to undermine the West's response to its war in Ukraine. For the Houthis in the Middle East, targeting subsea infrastructure in the Red Sea is a low-cost, high-impact form of attack. Europe needs to better prepare for this kind of accelerating warfare by increasing the resilience of its offshore and subsea infrastructure. It also needs to build societal resilience against the effects these attacks could have on social cohesion.

Attacks on offshore and subsea infrastructure are not new, but they are becoming more common. A year after the Nord Stream pipelines sabotage of September 2022, attacks on the Balticconnector pipeline drove European gas prices up by 12.5%.[3] Damage to four subsea cables in the Red Sea earlier this year impacted 25% of communications traffic between Asia and Europe, and the Middle East.[4]

These examples highlight the vulnerability of offshore and subsea infrastructure. While countries in Europe and North America have been vigilant about cyber-attacks for a long time, the vulnerability of physical infrastructure such as pipelines has become a prominent concern more recently. Offshore and subsea infrastructure is essential for energy supplies and global communication.

THE VULNERABILITY OF ENERGY INFRASTRUCTURE

The sabotage of the Balticconnector and Nord Stream pipelines highlighted the vulnerability of pipelines, and with that the vulnerability of nations' energy security. As Europe reduced its dependence on Russian energy in the wake of the invasion of Ukraine, Norway became the continent's most important source of energy. As a result, it also became a more significant vulnerability. If Norwegian energy infrastructure or gas distribution networks were to be disrupted, prices would rocket, and Europe would struggle to find an alternative gas supplier quickly.

There are indications that hostile actors are watching energy infrastructure in Europe closely. In 2022, multiple unidentified drones were seen flying near Norwegian oil and gas platforms, triggering a military surveillance response.[5] Dutch intelligence services have warned of Russia mapping gas pipelines and wind farms in the North Sea as potential targets.[6] The impact is psychological as much as physical. Energy companies are concerned not just about attacks on their infrastructure, but also that their employees may become reluctant to travel to platforms if they fear for their safety with increased attacks on the infrastructure or the helicopters used to transport them.

"Energy companies are not only concerned about attacks but are also worried workers may become reluctant to travel to platforms to work because of them"

THREATS TO COMMUNICATIONS INFRASTRUCTURE

As for communications infrastructure, as the world has become more connected, and the global economy has become digitised, subsea communications cables have also gained prominence as strategic assets. They are essential for global internet traffic and financial transactions. At least 99% of the world's digital communications travel through the subsea cable network.[7] Military and intelligence agencies also rely on these cables for intelligence gathering, although the ease of doing this has been overstated.[8]

The threat here is two-fold: first is the impact of sabotage on global digital connectivity, and second is the risk of espionage. As there is no viable alternative to these cables for data transmission, any attacks have the potential to be high impact.[9] When it comes to espionage risk, Russia clearly is not the only adversary the West should be concerned about. Subsea cables are largely laid and owned by the US, France and Japan. China has tried to break into the market but has largely been unsuccessful.[10] Yet a cable is most at risk when it is repaired following a fault: hostile actors can exploit the opportunity to install data extraction devices for espionage purposes.[11] In instances of faults on US cables in recent years, repairs were carried out by a Chinese engineering company.

THE WEST NEEDS SOCIETAL RESILIENCE

The risk and impact of the threat to energy and subsea cable infrastructure are clear. NATO, the EU, individual European countries and the US have responded with a flurry of initiatives aimed at increasing resilience, detecting suspicious actions and responding to incidents. Safeguarding energy and telecommunications security is now as important to national security as deterring hostile states and counter-terrorism efforts. Ultimately, however, the biggest priority has to be building resilience against these threats, both in the event of physical attacks on infrastructure and in fostering societal resilience should they occur.

[1]UK Government 'Pervasive pattern of hacking'; Chatham House 'Hybrid warfare on the EU'; The Economist 'France uncovers vast Russian disinformation campaign'; Euronews 'European hospitals targeted by pro-Russia hackers'; NATO 'Countering hybrid threats'
[2]University of Reading 'Non-state actors in hybrid warfare'
[3]CEPA 'New attack on Europe's energy pipelines'
[4]CNN 'Red Sea cables have been damaged, disrupting internet traffic'
[5]Reuters 'Norway oil safety regulator warns of threats from unidentified drones'
[6]Politico 'Russia 'mapping' critical energy infrastructure, say Dutch intelligence agencies'; Ministrie van Defensie (Netherlands) report
[7]European Parliament 'Security threats to undersea communications cables and infrastructure'
[8]The Guardian 'GCHQ taps fibre-optic cables for secret access to world's communications'
[9]CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence) 'Strategic importance of, and dependence on, undersea cables'
[10]Financial Times 'How the US is pushing China out of the internet's plumbing'
[11]Financial Times 'How the US is pushing China out of the internet's plumbing'

RISK MANAGEMENT

Investment Manager Jamie Zegleman explains why the concept of resilience matters so much to the team at Walter Scott

As long-term investors we aim to be cognizant of all the material risks that might face the companies in which we invest. Yet there are always risks that are hard or even impossible to identify. Further identifiable risks may be deemed unlikely, but such risks do, on occasion, materialise. So we look for companies which are able to deal with the unexpected. To tackle this challenge, our research process seeks to identify as many of the specific risks to a company as possible, through rigorous research and informed team debate.

For those less stock-specific and less identifiable risks, our philosophy provides protection. Corporate resilience is, we believe, built into the companies in which we invest as a result of the characteristics that are central to our investment framework.

Amongst others these include diversification (by geography and end market, and with regard to supplier and customer concentration), financial resilience (strong balance sheets, strong profitability, high levels of pricing power and low demand cyclicality) and robust organisational structures and governance (which support contingency planning and give companies a better chance of responding successfully to unexpected shocks).

With these attributes in place we saw, in many instances, remarkable resilience in the face of the lockdowns and disruptions that stemmed from the Covid-19 pandemic. As companies have contended with increased interest rates and inflationary pressures so too those companies with financial strength and market leadership have not just coped but often prospered.

More recently geopolitical issues and military conflicts have very regrettably risen up the list of risks that we must consider. With war on the border of Europe, we have become increasingly aware of the impact of events closer to home. As well as the human impact of the war following Russia's invasion of Ukraine, we have seen disruption to Europe's oil supplies and inflationary worldwide shortages of grain. While these eventualities might have arguably been foreseeable, others are less obvious.

Warfare comes in many different guises.

IMPORTANT INFORMATION

This article is provided for general information only and should not be construed as investment advice or a recommendation. This information does not represent and must not be construed as an offer or a solicitation of an offer to buy or sell securities, commodities and/or any other financial instruments or products. This document may not be used for the purpose of an offer or solicitation in any jurisdiction or in any circumstances in which such an offer or solicitation is unlawful or not authorised.

STOCK EXAMPLES

The information provided in this article relating to stock examples should not be considered a recommendation to buy or sell any particular security. Any examples discussed are given in the context of the theme being explored.

WALTER SCOTT & PARTNERS LIMITED, ONE CHARLOTTE SQUARE, EDINBURGH EH2 4DR
TEL: +44 (0)131 225 1357 · FAX: +44 (0)131 225 7997
WWW.WALTERSCOTT.COM

1.1_COM001814_27/05/2024