DEFENCE AND SECURITY FORUM

21 CLOUDESLEY ST
LONDON, N1 OHX
00-44-207-837-9212
M 00-44-7778-917133
Email olga.maitland@virgin.net

3rd CISO 360 MIDDLE EAST CONFERENCE
15th November 2021
HABTOOR GRAND RESORT,
DUBAI

Cyber Security Leadership

Lady Olga Maitland,
Advisory Board Audere International
President, Defence and Security Forum

PROTECTING NATIONS

The conference is all about giving leadership in the business sector. Quite rightly, businesses have every right and expectation that while they have individual responsibility to protect their enterprise, there is one body above, who have a duty of care for the safety of a nation against cyber-attacks, and this in particular applies to the military.

A country that is safe and at peace from any form of attack will naturally prosper.

Threats to a nation used to mean, an all out war, with traditional military hardware from tanks to battleships to fighter aircraft.

And it was easy to see the enemy. He was there in front.

World War 1 and World War 11 were German invasions into neighbouring countries. In the Iran Iraq war and the Gulf Wars of the 1990s, Saddam Hussein invaded with tanks. You knew who the enemy was – and squared up accordingly.

Today, we have **grey** wars. Some call it hybrid wars. Cut and run attacks as in eastern region of Ukraine, insurgencies, insurrections, stirring up regions to breakaway from a host nation, as with Crimea. 2006 the Israel Lebanon conflict, where Hezbollah used a host of new tactics against Israel, including innovative technology.

And now a new enemy – a cyber-attack on military and critical civilian infrastructure. Invisible. No idea where it comes from. Awesome power to destruct and disrupt. Above all, no international protocol or agreements to manage the threats. No one to negotiate with or will admit to. We are aware that nation – states cyber-attacks are common often using third parties or non-state actors in the process.

As Australia's Defence Minister Linda Reynolds said,' *What is clear now, is that the character of warfare is changing, with more options for pursuing strategic ends just below the level of traditional armed conflict'...*

Not just a matter of promoting insurgencies but interfearing and manipulating governments elections

And with it the tool, is technology, a cyber-attack. Vladimir Putin, Russia's President warned that whoever leads in AI and with it cyber will dominate the world.

For Russia it is war on the cheap. A broken economy means they cannot afford a conventional war. But using the invisible cyber intervention, it can mean massive disruption with modest investment rendering manpower and hardware to second place. The targets are a mix of military data and software and civilian government infrastructures, public opinion and election campaigns, against difficult to prove the source.

When challenged, Russia of course denies any involvement. How can you prove it? But we have a strong idea where they come from. Examples include Russia's cyber disruption of the Ukrainian power supply in 2015.

Russia's cyber governance is under President Putin's personal control. For the moment they are not equal in power and skills with the US and have not reached the top end surgical cyber capability, but for all that do have a ruthlessness to use it as a tool, and do not hold back.

They have no hesitation is backing non-state hackers to do the job for them. Such as in March 2011 the hackers who took over the websites of Poland's Atomic Energy and Health Ministry to spread false alerts of a non-existent radio-active alert.

The same month both Russian and Chinese intelligence services targeted the European Medicines Agencies stealing documents related to COVID vaccines and medicines.

There are attacks designed to cause significant economic disruption, targeting companies or whole sectors. The Iranian attacks disabled 30,000 computers belonging to Saudi Aramco in 2012, let alone their attacks on multiple US financial institutions - surely examples of gathering storms,

The Iranians attacked Israeli water treatment plants last year.

15 years ago, Estonian banks, media outlets and government bodies were struck down by cyber-attacks.

Even with these examples, and they are just examples, we have not yet begun to grasp the full impact such attacks could have on future warfare and geopolitical instability. As it is, tensions between US and China are volatile which only raises temperature all round, and a tendency to prod the other side.

Henry Kissinger, 98!!!!, in a recent interview to the FT began his life at the time of nuclear weapons expansion in the 1970s. It was a case of the US versus the Soviet Union. Kissinger said, 'Each side eventually acquired knowledge about their nuclear capacities and doctrines that may be impossible to match with cyber using A1. There is no clear way of deterring attacks, or of knowing where they are coming from'.

Artificial Intelligence is an added tool to cyber security and helpful to under resourced security operations.

Kissinger added 'If an unrestrained US-China arms race goes from nuclear to AI, the dangers of dramatic escalation would be very great'.

What is relatively new are undeclared adversaries, state and rogue non-state actors exploiting information technologies and testing vulnerabilities – businesses, state systems and infrastructure being key.

`. It is getting more complex and unlike nuclear weapons cannot be detected.

Above all there is an absence of global regulation. A nation's strength in AI and cyber capability is becoming increasingly intertwined in geo-political understanding.

Potential issues are:

- A new arms race due to proliferation of AI and cyber technology in weapons systems

- Creation of global mistrust, hindering global co-operation

- Effect on National Sovereignty as non-state actors also hold AI cyber resources

Potential challenges therefore are

- Absence of clarity on what is AI and ‘what we intend to do’ among policy makers

- There is a higher IP theft vulnerability due to software-based nature of AI systems.

- Technology cannot be completely controlled or held accountable.

AI has a dual use both by military and civil applications. Controlling the flow of such technologies is extremely difficult. There are no Rules of Engagement. Hence the vulnerability of Air Traffic management systems as one example.

A potential threat would be cyber-attack hitting a system controlling hazardous chemicals.

The common thread in all threats are cyber-attacks designed to bring down a nation and render defence systems useless.

Another element is the **response**. In the case of Israel who experienced a cyber-attack which they knew came from the Gaza, they responded with missiles which demolished a whole building and killed people inside.

Things have indeed changed.

The consequence is that Major governments around the world are adapting. As the Deputy Secretary General, NATO said, 'We cannot fight wars with the tools of the past. Traditional resources of ground forces and hardware have a role, but there are new elements in hybrid warfare which include cyber-attacks.'

In the UK, there has been a technological revolution at the heart of National Security. The Government has dedicated £1.5b to setting up a National Cyber Force to respond with 3,000 online experts, a mix of military and civilian expertise.

The NCF, National Cyber Force's aim is to deter and defeat criminals, terrorists and hostile actors who conduct espionage, sabotage, and subversion. In essence disrupt adversarial networks who threaten government departments, agencies, and critical infrastructure. An example would be to disrupt an enemy's air defence network. WE have seen the US disrupt an Iranian missile system, and that Israel disrupted Syrian radars in support of an airstrike.

There has always been a requirement to jam enemy communications on the battlefield. The difference today is that communications are digital, and internet enabled as opposed to high frequency radios.

A key ethos is to co-operate with allies, for example here in Dubai, the UAE with whom there is a close relationship. The purpose is to be strategic with focussed disruption rather than indiscriminate attacks having a mass effect.

Among the NCF's concerns will be our space-based intelligence, navigation, and radar which all modern military engagements rely on.

Alliance troops depend on a reliable satellite geometry and receiver system. However, during a NATO exercise in Finland, Finland’s civilian air navigation services were disrupted through electronic means., later attributed to Russia.

Loss of navigation capability was also reported in Norway at the same time. While not strictly cyber-attacks they illustrate the vulnerability of navigation systems to interference. And it will not stop there.

Space based tracking and surveillance systems are vulnerable to cyber. At present the US military cyber activity is heavily dependent on its space assets, since the vast majority of military cyber activity is conducted from outer space but although the combined China and Russia satellites are only a third of the US strength at present, they are frantically playing catch up and even with today’s capability can inflict huge damage.

All round, Sophisticated cyber-attacks on military systems may have operational and strategic consequences that change the way the military operates in conflict.

Tanks, aircraft, battle ships, all have software which drive them.   Intercept or disable them with cyber, they are rendered useless

Cyber-attacks could have a paralysing effect on strategic military and political decision-making and could render NATO countries vulnerable to Russian or Chinese information and deception operations.

We are now seeing the evolving *Digital Great Game* that is playing out of China’s Digital Silk Road and will probably be the most influential element of the Belt and Road Initiative.

They have also harnessed technologies and tactics that have outpaced international law. China’s new Strategic Support Force is designed to achieve dominance in the space and cyber domains. Digital Authoritarianism sums it up. And President Xi is determined to remain the most dominant power.

Hence the UK investment in the National Cyber-Force. In effect a regiment of 2,000 dedicated solely to cyber security, with boots on the ground reduced from 80,000 to 70,000 offsets the costs.

As the Defence Minister Ben Wallace said, ‘This is a counter-balance to adversaries who are investing heavily and using what we would call sub threshold to constantly attack us.’

The plan is to provide the option to ‘launch offensive cyber – weapons against adversaries or against other areas that currently pose a threat.’

The Chief of Defence Staff, Gen. Sir Nick Carter has warned that there is a real risk that covert cyber warfare could escalate into an ‘uncontrollable state of all-out war…’

Consequently, the dependence on spaced based technology is critical which when threatened by a cyber-attack can affect global positioning, reconnaissance, intelligence, surveillance, missile defence, communications, early warnings of a missile launch, providing precise locations for weapons strikes, and so on.

Precision guided missiles are dependent on information sent by satellites.

The risk is to misinterpret commands, or to lose contact with command centres and thus fail in operation.

Technology therefore is at the core of defence, not on the periphery. Final thought: old weapons systems could take up to 25 years from conception to deployment. Cyber-offensive tools are constantly and rapidly changing. More than that, infinitely cheaper to use.

Corporates have a responsibility to protect against cyber-attack. Meanwhile, Nation states have a responsibility to be in the front line accepting that their duty is to be the first line of defence.

SO how does the picture look in the Gulf and the region as a whole.?

The biggest threat comes from Iran: They regard themselves as being in an intelligence and cyber war with its enemies, especially Israel, followed by US and Gulf states. They did experience a big hit when the US with the help of a disaffected Iranian in 2010 targeted the principal uranium enrichment facility. Broadly Iran does not have highly sophisticated cyber technology but what they have they use to quite some effect.

North Korea. You would have thought they are a serious challenge. In fact, isolation has meant they lack any sophisticated cyber knowledge but make up for it by opportunism.

In the Gulf, The Emirates take the threats seriously.

Hard to say they are resilient to a large-scale cyber incident, as experienced y Saudi Arabia with the Iranian cyber-attack on Aramco. And indeed, the main threat has come from Iran targeting government agencies, foreign ministries, and intelligence agencies. But consequently, the GCC governments are investing heavily in cyber defence and collaborating with friendly countries like the UK

In the region India despite its geopolitical importance, has made only modest progress in developing its policy and doctrine for cyber security. The government may be slow and cumbersome, but the large talent pool in the private sector has moved much more quickly in promoting corporate cyber security.

Malaysia, however, is a mover and shaker and holds up well with many other countries. Totally committed to a national cyber security agenda with strong digital economic potential. Add to that they have close working relationships with UK, Australia and Singapore.

Vietnam. The ruling Communist Party have put in place a suite of cyber security strategies including the military domain which is part of their authoritarian system. They tend to focus more on the internal security for political reasons and have considerable ambition and potential. They do lack skills and resources, but through one of their government agencies they are capable of launching a relatively sophisticated cyber-attack.

Indonesia. At present for a country which is expected to become the fourth largest economy by 2030, its cyber protection programme is sluggish with limited capabilities. At present domestic orientated. But if the Government decides that the strategic circumstances demand it, then there will be greater investment in the cyber domain,

Japan. Despite being a world leader in the commercial application of information. They had a slow start in raising the importance and profile of cyber defence management. But the 2020 Olympic Games last year propelled them to a more robust cyber posture, prodded by the US and Australia as the threats from China and North Korea emerged.