# *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***





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


**Bosphorus Summit,**
**Conrad Hotel,**
**ISTANBUL**

**Monday 5th December 2021**

**PROTECTING NATIONS**

## A CALL FOR AN ARMS CONTROL AGREEMENT ON CYBER MILITARY WARFARE

A conventional war with military hardware was where it was easy to see the enemy. He was there in front. World War 1 and World War 11 had a clear enemy, the German military might.

. 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.

**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 interfering 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 for months 30,000 computers belonging to Saudi Aramco in 2012. This was the biggest and most damaging hit so far, in terms of cost and destruction.

Add to that the attacks on multiple US financial institutions - surely examples of gathering storms,

The Iranians used cyber to attack an Israeli water treatment plant 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 of many, 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 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.

AI has a dual use both by military and civil applications. Controlling the flow of such technologies is extremely difficult. Hence the vulnerability of Air Traffic management systems as one example.

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

**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 to disrupt adversarial networks who threaten government departments, agencies, and critical infrastructure.

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

Now the head of the UK Secret Intelligence Service, MI6, Richard Moore has declared that they too are investing in cyber protection.

As he said last week, ‘there is an exponential growth of online threats…our adversaries, such as China, are pouring money and ambition into mastering artificial intelligence, quantum computing and synthetic biology because they know that mastering these technologies will give them leverage.’

The aim in the UK is both defensive but also to launch offensive cyber weapons against adversaries or against other areas that currently pose a threat; disrupt an enemy’s defensive mechanism such as their air defence network. WE have seen the US disrupt an Iranian missile system, and that Israel disrupted Syrian radars in support of an airstrike.

The UK key ethos is to co-operate with allies in NATO including Turkey, and friendly countries who share our values.

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. 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.

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.

Not surprising therefore that Turkey is also investing in cyber protection with the launch last year by the President of the National Cyber Security Intervention Centre.' Turkey, like all of us, has experienced its own attacks by malware and recently on the municipality of Konya when 1m people's private data was stolen.

Conclusion: 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 – and very potent.

*The time has come therefore to establish an arms control/protocol and curb the very destructive threat cyber military warfare presents. We have no time to lose.*