The Cyber domain; Everything affects everything – the cyber domain and the Grey Zone

By Nick Watts

THE FIFTH DOMAIN - CYBER

In 2010 the advent of 'cyber war' was claimed to be the Fifth Domain of military operations. The others being Sea, land, air and Space. Subsequently military planners and national security personnel have worked hard to ensure that the cyber domain is understood by the armed services and national security agencies, both the threat and the possibilities. But looking at the cyber domain in a silo is to fail to understand how the advance of technology will impact on our security at home, as well as the capability of our military forces to be effective in the face of a rapidly changing threat.

Since 2013 the EuroDefense Working Group on cyber security (now an observatory) has monitored developments in this domain, and the response of policy makers at the European level. The EU, NATO and national agencies have made adjustments to ensure that legislation is adequate to ensure that citizens' rights are protected, that our Critical National Infrastructure (CNI) is safeguarded, and that law enforcement agencies have the tools to pursue cross border crime and terrorism. The cyber domain is now an integral part of both national defence and security, as well as an enabler of much of the digital economy, on which our prosperity increasingly depends.

The advent of quantum computing and Artificial Intelligence (AI) added another layer of potential threat, or opportunity, which policy makers were just beginning to grapple with. The onset of the war in Ukraine, begun in February 2022, has changed the discussion from the academic into a recalibration of how to counter the threat from state on state warfare. An early lesson seems to be that all the military domains are now an integral part of statecraft. Thinking in silos is a recipe for defeat.

Matters have now come into sharper focus. Autocratic regimes have identified the internet as a potential 'Trojan horse' that would allow the free flow of views and information, to their disadvantage.

They have sought to shut out the 'free world' through filters such as 'the great fire wall of China'. At the same time, it is a tool which can be used to spread disinformation. The cyber domain is now an essential enabler of so called 'grey zone' operations.

THE GREY ZONE

The phrase 'grey zone' refers to activities undertaken by a state which are deniable, and at a level below that of actual armed conflict. The difference between this and terrorist campaigns, is that they are directed by a national capital rather than a separatist or ideologically motivated group. It is the vulnerability of infrastructure managed by the private sector such as fibre optic cables and pipelines under the oceans, part of the global commons, which poses a risk to open societies.

The advent of social media means that more people now receive their information and opinions from internet platforms managed by large corporations interested in harvesting the users' personal data for commercial gain. Calls from governments to monitor the content have sparked debates about freedom of speech.

GERASIMOV DOCTRINE

The term 'Gerasimov doctrine' was first coined by Mark Galeotti in 2013, referring to the approach he identified being applied by the Russian state to counter the technological superiority of NATO and the west. Having seen how the US led coalition conducted operations in the two gulf wars and in the Balkans, the Russian general staff understood that the best way to counter what it believed to be hostile western influence was to engage with it at every level. Many commentators drew parallels between the Gerasimov doctrine and a similar approach being adopted by the Chinese military. A key element of this was the information space.

The Russian incursion into Crimea and the Donbass region of Ukraine in February 2014 is recognized by many as the first overt manifestation of this kind of military operation. Subsequently Russia pursued a campaign of cyber-attacks against Ukrainian infrastructure. Paradoxically, this behaviour gave the west a good insight into Russian methods, and how best to counter them. The information campaign conducted before the February 2022 attack seems aimed mainly at bolstering public opinion inside Russia.

A2AD

China has been pursuing a similar approach to what it sees as western encroachment into its sphere of influence. Its main focus has been a military build-up in the South China Sea, combined with incremental land grabs of what it sees as strategically important islands. It has also been using its economic strength and the offer of financial assistance with infrastructure development in the global south to counter western influence. Its Belt and Road initiative is seen as a counter to the 'Washington consensus' whereby western aid and development is accompanied by demands for reform of political and economic structures internally.

Both Russia and China have pursued a military strategy defined as Anti Access Area Denial (A2AD) by which their adversaries are kept at strategic distance by the threat of precision munitions. In this sphere the new arms race is about developing and countering hypersonic missiles. The west has sought to counter this with the 'Third Offset Strategy' announced by US Secretary of Defence Chuck Hagel in 2014.

This was intended to galvanise the defence sector into embracing the innovation necessary to counter the A2AD capabilities of China. But the campaign in Ukraine reminds us that warfighting still requires the use of infantry, armour and especially artillery.

MULTI-DOMAIN OPERATIONS - FUSION

The Western response to both the A2AD challenge and Grey Zone warfare is perhaps best seen in the UK's Fusion doctrine, which resulted from the National Security and Capability review of 2018. It seeks to harness all of the elements of statecraft into an all-government approach to defence and security.

Whilst the main emphasis for this particular policy is on defence and security as well as diplomacy and development policy, it should be remembered that the key vulnerabilities in open societies remain areas managed by the private sector. A truly comprehensive approach would

embrace a resilient civil society, with the public engaged in thinking about their own personal security. The Skripal poisoning in Salisbury in 2018 resulted in one death, but also in huge disruption to the citizens of the city. Similarly, the Litvinenko poisoning in 2006 resulted in a large scale health emergency in the heart of London.

The challenge facing policy makers and senior military planners is where to place their bets. In an autocratic regime public opinion and public finances are not a consideration. Opinion whipped up by a centrally driven doctrine can be easily amplified by social media. Western agencies can monitor and report on these developments. The response to Russia's attack on Ukraine was to harness the power of sanctions to deny market access to Russian commerce and finance. Sustaining this campaign will require good messaging by governments. Both NATO and the EU are adapting to respond to the lessons learnt from the campaign in Ukraine, but it is the taxpaying citizens who are footing the bill, as they face increased energy and food costs.

Propaganda and disinformation are not new, but the development of AI powered platforms means that the information space is contested. This is why a strong civil society needs protecting. It is our communities and institutions – the ones that we hold dearest, that we trust and rely on, that make our lives worth living. The public are not stupid, they don't need lecturing, but it is helpful to be reminded of the things that bring us together – whether that is the Eurovision song context, or the champions' league. Service personnel are as tribal as football supporters, when it comes to defending their own services, but the future character of conflict will require more joined up thinking and operations.

There is a widely quoted saying: 'everything affects everything' this is certainly the case in the sphere of military operations and especially so in the cyber domain. The time is past for old style thinking in silos, it is comfortable for bureaucrats and those who seek to safeguard their departmental budgets. But the enemy gets a vote too, Grey Zone operations mean that the west must be agile and innovative. Sharing best practice among allies, exemplified by the NATO Co-operative Cyber Defence Centre, will enable the sharing of information.

The advantage enjoyed by civil society over autocracies is the avoidance of group think, which appears to have weakened Russia's campaign from the outset. But we must continue to share and develop new ideas. A network such as EuroDefense has a variety of experience and expertise it can access, such as the work done by our various Working Groups, the output of which can be fed to European institutions.

The Grey Zone is an area that deserves more light being shone upon it, so that we and our fellow citizens can be well prepared and protected.

Nick Watts is the Vice President of Eurodefense-UK and rapporteur for the Eurodefense Cyber Observatory