CYBER THREATS TO NATO

Professor Sir David Omand GCB
War Studies Department, King's College London and former UK Security and Intelligence Coordinator, Cabinet Office, Director GCHQ and Deputy Under Secretary of State for Policy, MOD London

I have been asked to address the subject of cyber threats to NATO. I interpret that as not just threats to NATO as an institution but also threats to the work of NATO through member nations engaged in NATO business and contributing forces to live NATO operations.

Let me start with an unchallengeable proposition. Any serious armed conflict in which advanced states participate will involve a cyber dimension. When NATO forces face a serious adversary then the NATO commanders will – must – have at the back of their minds the worry that the adversary will succeed in blunting some of their capabilities. It might be that satellite communications systems, GPS, air defences or a C4I system will not work as expected or in the future, who knows, it may be that weapons systems and their sensors cannot be relied upon to function as they should because of adversary cyber action, including trojan attacks inside key software – or in the future – hardware that is activated when hostilities start.

The security problems for those that design, manufacture and maintain complex electronic systems are hard. There will be no sure way of providing the level of assurance in future that a NATO commander would have today that it will be all right on the night. There are mitigating steps that can be taken in the design of new weapons systems, such as using mathematically sophisticated methods for writing secure code. Manufacturing can be in-sourced to secure facilities inside some NATO member states. Restrictions can be imposed on which countries may supply weapons systems components to NATO nations.

Redundancy can be designed into communications systems that can be architected to continue to function even when degraded. And so on. There is only one certainty. Such measures will push up costs. The cost of consumer digital devices and apps may be falling but the costs will rise of the specialised forms of these technologies that have to be guaranteed to work under very hostile conditions. And more intensive personnel vetting to guard against the insider attack will become even more important than it was during the Cold War and that will add cost too.

If what I have just described looks difficult then you would be right. But that is the easy part of dealing with the cyber threat to NATO since it relates directly to military capability itself. The cyber threat to NATO is very much wider than that. A second preliminary remark is to point to the dependence of modern armed forces on digitised information. It is in the nature of such information that it can not only be stolen, but denied, altered and corrupted – and we might not know that in time.

> “”
> The security problems for those that design, manufacture and maintain complex electronic systems are hard. There will be no sure way of providing the level of assurance in future that a NATO commander would have today that it will be all right on the night

Which brings me to a third preliminary remark, that modern armed forces are more dependent than ever on the functioning of the critical national infrastructure on which everyday life depends such as power, communications, and logistics. Most of the infrastructure is in the hands of the private sector and not under government control. NATO's defence capabilities are dependent on the proper functioning of tens of thousands of digital systems over which neither NATO nor the NATO nations have much, if any, control.

In the old days, there were elaborate war books with plans on which NATO mobilisation and transition to war would depend, taking ships up from trade, commandeering roll-on roll-off ferries and protecting the critical infrastructure nodes from sabotage. Today's digital world is very different.

I have an acronym to describe the wider range of cyber threats from hostile states and non-state actors to which NATO and NATO nations, companies, and citizens are now exposed: CESSPIT [Crime, Espionage, Sabotage and Subversion Perverting Internet Technology].

Credit: Markus Spiske on Unsplash

These threats are getting worse and are persistent. In the cyber domain the absence of war does not mean the absence of conflict. Let me therefore look at the relevance of that new threat environment, what has been called the grey zone, to NATO as a functioning Alliance. I start with crime. We are all aware of the rise in cyberattacks for illegal gain, with a low risk of being caught, the ability of criminals to base themselves in countries with no extradition treaties, and the generally lower penalties for what is seen as a white collar crime that does not put the public in direct danger. NATO has many administrative systems. They handle payments and receipts, and are therefore a target in the same way as in every company or government department. The response has to be to adopt the same cyber security measures as other large complex organisations, including attention to the people dimension given the insider threat.

When defence industry improved their corporate IT systems, criminal groups and hostile states started to attack their legal advisers, their auditors and the small- and medium-sized enterprises in their supply chain since they were likely to be less well defended yet still had digital connectivity with the high value target. We also know that in the case of Russia, criminal groups are used by state intelligence agencies as hackers for hire. Even administrative systems for NATO could therefore represent security vulnerabilities.

Which takes me to the next letter in the acronym, E for espionage. When it comes to the digital espionage threat, NATO is a target three times over. NATO is first of all an important international organisation and therefore attracts attention from the intelligence agencies of a very wide number of countries, all of which maintain capability in Brussels. The head of Belgium's domestic security service was reported a few years ago as saying that Brussels had taken over from Vienna the title of spy capital of the world, given the very large number of diplomatic targets and international organisations located there. The list of attackers extends well beyond the obvious rogue states.

We should remember the military maxim that you attack where the enemy is most vulnerable not where the enemy is strongest. The hostile intelligence agency will look to target those member states whose cyber security is relatively less advanced than others. And to recruit agents similarly, who may be able to facilitate digital access. That is another big difference with the pre-digital age of the Cold War. Once inside, the attacker will spend months moving laterally round the system trying to locate the really valuable information and acquiring the access permissions and passwords to access it. And at that point it is not just a few key documents that are covertly purloined but the whole database. It is all stolen, as Edward Snowden's thefts from NSA remind us. A second characteristic is that NATO has the United States at its heart, including its nuclear capability declared to NATO. For nations such as Russia, China, Iran and North Korea, NATO and its member states represent a route into gathering information about the US defence community. A third reason for NATO to be a major intelligence target is that it is an operational organisation that potential adversaries need to study closely in order to identify capabilities, orders of battle, command structures and all the C5I processes that support them.

In Cold War days, espionage against NATO and the NATO nations was a given. But all that peacetime hostile intelligence activity against NATO could be kept in a different conceptual box from the threat of aggressive use of armed force against the NATO area which the NATO strategy of defence and deterrence successfully contained. That is not possible in today's digital world. The difference between today's cyber intrusion into a computer system for the purpose of espionage and a cyberattack intended to destroy or degrade that system is only few lines of code. The intrusion and subsequent exploration and mapping of the network may be for the purpose of intelligence gathering, or it may be to conduct immediate sabotage, or it may be to plant malware for later activation, for example in the event of hostilities. You cannot be sure. Nor will we always be as certain as we would want to be who conducted a cyberattack when we discover it since the ways of creating false flags on attacks is getting more sophisticated. Attribution will be hard.

> “”
>
> Attackers pick the weakest link in the chain, so NATO must work with the cyber security organisations in member states to raise everyone's game, drawing on the experience of the nations that are furthest ahead in devising and implanting national cyber security strategies

My next letter in the acronym is S for sabotage. The cyber threat to the critical infrastructure of NATO nations is well recognised. A recent example shows the destructive potential of sabotage attacks, the Russian NotPetya worm was released to cripple targets in Ukraine but escaped. It infected companies around the world including the logistic systems of Maersk, the world's largest shipping conglomerate. The company was within minutes of losing the global systems that record what is in each container, where it presently is and where it is going. Without that knowledge even a giant hyper-efficient company dies, and dies quickly. Maersk has estimated the cost of this Russian cyberattack at between $250-300 million. The lesson for NATO and Western nations of the sabotage threat is clear.

It is a hard problem to defend infrastructure since much of it is in private sector hands and it is civil government that has the largest role in advising on peacetime cybersecurity. But as I have already pointed out, attackers pick the weakest link in the chain, so NATO must work with the cyber security organisations in member states to raise everyone's game, drawing on the experience of the nations that are furthest ahead in devising and implanting national cyber security strategies.

The fourth letter is S for subversion. An examination of Soviet subversive activity directed against NATO nations during the Cold War shows that there are three key components: intimidation of the victim; hostile propaganda directed at the victim, at the international community to warn them off interfering and at the Russian domestic audience; and 'active measures' otherwise known as dirty tricks, such as using covert agents of influence, spreading anti-Western rumours and planting forgeries and fake stories. All these three components of subversion can now be carried out more easily and cheaply using digital means. Russia has continued the Soviet tradition and is active in directing such digital subversive activity against NATO as an institution (for example over forward deployments) and against NATO nations (for example the interference with the 2016 US election and the disinformation campaigns in Europe stoking tensions over immigration and trying to undermine sanctions on Russia over Ukraine).

What should NATO do? In brief, establish common situational awareness of everything that is going on by way of cyber threats against NATO and NATO nations; agree a NATO-wide cyber security strategy that addresses all the vectors of threat; build programmes of action to enhance cyber defence of NATO networks including recent developments in active defence (as is being used for the UK government sub-domain, .gov.uk). It will be essential to address human as well as technical aspects of security; and engage in mutual support to ensure all NATO nations reach the standards of the best.

All of that contributes to 'deterrence by denial' by making NATO a harder target. In addition, there is deterrence of potential adversaries through the threat of offensive cyber capability that a number of NATO nations have already said they are developing. Comparisons with the role of nuclear weapons in NATO strategy would be highly misleading. But we should think about mechanisms within the Alliance for planning and consultation on the role of offensive cyber in Article V circumstances (including where there is loss of life and damage equivalent to an Article V armed attack).

I would expect the nations that possess offensive cyber capability to reserve to themselves final decisions on use (where there is a parallel with the nuclear weapons declared to NATO) but there needs to be understanding of the general nature of the capability, and integration of this component of warfare into strategy and doctrine for the major NATO commanders (again perhaps some read across to the pioneering 1960s work of the US chaired NPG staff group). Such consultative mechanisms might then take on the task of building NATO doctrine for response to peacetime cyberattacks below the threshold of armed attack. What we can be certain of is that there is plenty here for NATO to work on over the coming years.