



CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org.uk
F: +44 (0)20 7957 5710 www.chathamhouse.org.uk
Charity Registration Number: 208223

Transcript

Cyber Warfare: Addressing the Challenge

Nick Harvey MP

Minister of State for the Armed Forces

9 November 2010

The views expressed in this document are the sole responsibility of the author(s) and do not necessarily reflect the view of Chatham House, its staff, associates or Council. Chatham House is independent and owes no allegiance to any government or to any political body. It does not take institutional positions on policy issues. This document is issued on the understanding that if any extract is used, the speaker and Chatham House should be credited, preferably with the details of the event. Where this document refers to or reports statements made by speakers at an event every effort has been made to provide a fair representation of their views and opinions, but the ultimate responsibility for accuracy lies with this document's author(s). The published text of speeches and presentations may differ from delivery.

Nick Harvey MP:

I would like to start by thanking Chatham House for giving me this opportunity to speak here today, and to commend Paul Cornish and his colleagues for their report launched this week *On Cyber Warfare*.

It challenges us to think in different ways about our approach to cyberspace.

It challenges us to bring the debate out of the technical realm and into the political.

The Challenge of Cyberspace

As a liberal, I am excited about the capacity of the internet and digital technology to increase the freedom and opportunity available to our citizens – to enhance people’s ability to control their own lives and make their own choices – and to expand their horizons.

But I also recognise that when it comes to cyberspace, the old adage that man is wolf to his fellow man has sadly proved itself correct once more.

Wherever he expands his dominance, whether it be on land, sea or air, or whether it be in cyberspace, mankind carries his essential nature with him.

As Minister for the Armed Forces, I am concerned with how we should defend ourselves against those who would use cyberspace to do harm, and how we best use the new technologies to further our national security.

For me this is about protecting people’s privacy and livelihood not diminishing them – this is about protecting the freedom and opportunity cyberspace brings.

But to do that we must recognise that the threats in cyberspace do not just come from malicious mischief makers or organised criminality.

Nor is it just our privacy and money that is at stake.

Most societies, including Britain, have come to rely on digital networks for many of the things which allow normal life to function smoothly.

It is at the heart of our transport system, our power and telecommunications, our health service and our economy as a whole.

We take these technologies for granted, and we have come to depend on the services they provide every second of every day.

The consequences of a well planned, well executed attack against our critical networks could be catastrophic.

The fact that cyber security has been identified as one of the top national security threats for the UK over the next five years indicates both the likelihood of such an attack and the level of impact.

Without doubt, man has brought the capacity for war to cyberspace too.

In order to protect ourselves we need to understand how cyberspace might be used.

We must apply the same kind of logic Clausewitz applied to the conditions of his age, when looking to formulate approaches to the conditions of our age.

As Clausewitz showed, while the essential nature of conflict is unchanging, its character moves with the times.

So I would like to look at the changing character of conflict and how this might manifest itself in the cyber domain.

The Changing Character of Conflict

As the coalition government's new National Security Strategy demonstrates clearly, Britain is today both more secure and more vulnerable than in most of our long history.

We are more secure in the sense that we do not face, as we have so often in the past, a conventional threat of attack on our territory by a hostile power.

But we are more globally interdependent, more networked and more reliant on digital technology.

These are sources of economic strength – but also of vulnerability - and this reliance may be our soft underbelly.

Those who would mean us harm - be they states trying to gain an advantage – or those driven by ideology or straightforward greed – may not have the capability to challenge us using conventional military means.

Instead they will seek to attack or undermine us in indirect ways – striking where we are most vulnerable – seeking to coerce us, to disrupt our society and do damage to infrastructure and people.

Over the past ten years we have seen civilian aircraft used as suicide bombs.

We have seen naval vessels attacked from inflatable dinghies.

We have seen the rapid evolution in the technology and tactical use of improvised explosive devices – against our armed forces in places like Afghanistan - against our citizens on the London tube - placed on planes, driven into airports – designed to cause as much death and destruction as possible.

This is asymmetry in warfare.

It avoids direct military confrontation; it avoids striking at strength and seeks to exploit perceived weakness.

The Asymmetrical Power of Cyberspace

The domain of cyberspace lends itself directly to this form of conflict.

Let me give four reasons why.

First, there is a low threshold of entry.

Our adversaries can exploit the same technology used by citizens going about their daily business.

That laptop that sits on the desk at home or in the office – used to do accounts, send email or catch up with television programmes – is the same instrument that could be used to launch an attack on our critical national infrastructure.

And the tools that would be used, the malware or viruses, are traded on the net – a black economy of rapidly growing size and sophistication.

In this way, a single networked laptop in the hands of a sophisticated and informed attacker could be as effective a weapon as, say, a cruise missile.

Second, there are no geographical barriers in cyberspace.

An attack could be launched from any corner of the world with little warning.

Unlike a conventional military movement - which requires the kind of organisation, mobilisation and logistical support that is hard to hide - a cyber attack can essentially be covert until the moment it begins to do its work.

Third, attribution of both cause and effect will be difficult to achieve.

As we already know from the recent STUXNET worm, it can be very difficult to trace from where and by whom an attack was initiated.

And it may be unclear when a cyber event is taking place, what its exact purpose might be or the ultimate aims of the attacker.

Fourth – and perhaps most insidious – with cyber it is possible to rapidly create a mass effect.

As we saw in the cyber attacks of Georgia in 2008 – hackers can be enlisted to ideological causes, equipped with the means to carry out mass attacks – so called botnets – and given the target information to direct and synchronise attacks.

Rather than a single attack on a target – this can result in hundreds of thousands of computers worldwide being hijacked.

As an example, last week Burma experienced a mass denial of service attack which effectively severed its internet connectivity with the rest of the world – just days before its first election in more than 20 years.

All this means that cyber is a powerful asymmetric tool for warfare.

We have seen how terrorists can attack symbolic rather than military targets - the 9/11 attacks on the World Trade Centre being an obvious example.

It can only be a matter of time before terrorists begin to use cyberspace more systematically, not just as a tool for their own organisation, but as a method of attack.

On Cyber Warfare

But cyber is also a powerful tool in the hands of those traditionally able to engage in conflict – states themselves.

As Iain Lobban, the Director of GCHQ, said recently: we have seen the use of cyber techniques by one nation on another to bring diplomatic or economic pressure to bear.

The digital age has also enhanced the effectiveness of our military operations - providing secure communication networks, accurate navigation, and the ability to synchronise and deliver precise effects at a time and place of our choosing.

So it is inevitable that we have seen the blending of conventional and asymmetric means to support the attainment of objectives.

Again, as I mentioned before, such attacks can be conducted from a 'safe' distance and makes the attribution of attacks more difficult.

Cyber attacks on Georgian infrastructure in 2008 by supporters of South Ossetian separatism coincided with the Russian military offensive.

These attacks created a 'fog of war' in which the Georgian government was unable to communicate with the international community to rally support to its cause.

The cyber attack had both a tactical and strategic effect on the Georgian state.

The integration of cyber and physical attack would seem to be the most likely use of cyber in the military sphere.

We must therefore win the battle in cyberspace, as well as the battle on the ground.

So the first thing we should recognise is that actions in cyberspace form part of the future battlefield, rather than being separate from it.

It adds a new and modern dimension to conflict, but what it seeks to achieve should be subject to the same strategic and tactical thought as a conventional military operation.

We will encounter the same adversaries with the same motivations in cyberspace as we do in the real world – albeit in a new environment which has its own unique characteristics.

As Clausewitz believed, war is an expression of politics by other means.

This means we should also be able to prevent, deter, coerce or even intervene in cyberspace.

This will not be easy.

There are those who argue that in countering cyber threats, conventional concepts will be rendered obsolete.

I have some sympathy with that view and we will need to adapt our analysis to the architecture of cyberspace.

But, I do not believe we should just concede that because it will be difficult to apply concepts like deterrence to cyberspace, that it will be impossible.

As I have said, cyberspace is a new domain, but it is still a human domain with all the actions there driven by human behaviour and motivations.

So we should not jettison centuries of proven learning in awe of the complexities – we should reapply them to the new circumstances and supplement them where necessary.

So let me turn now to how we are doing this and the work of the coalition government and others to integrate cyberspace into our thinking on national security.

Cyber Security

Our National Security Strategy recognises that the response cannot, and must not, be for government alone.

There is no on-off button that government can use for our national networks and there is no defined perimeter in cyberspace which government can defend.

We must draw more effectively on the knowledge, experience and resources of the private sector who own and operate large parts of the critical networks that deliver our essential services.

Our national approach to cyber security must be sophisticated.

It requires us to keep pace with new technologies.

But reducing vulnerability requires an understanding of people's behaviours as much as it does network topology.

It means understanding what is critical to protect and managing the risks.

We will need dynamic defences that are able to - first, identify and assess risks - but second trace events to their source and stop them.

While government must lead – cyber security can only be delivered as a partnership between government, industry and academia.

That is why the Strategic Defence and Security Review has launched a transformative National Cyber Security Programme supported by £650m of new investment over the next four years.

This will overhaul not only our approach to tackling cyber crime, but also the UK's ability to defend itself from cyber attack.

And it will seize the opportunities which cyberspace provides for our future prosperity and for advancing our security interests.

In the UK, as I have suggested, we have strong capabilities on which we must build.

These include protecting our critical national infrastructure, protecting the operations of our armed forces at home and abroad, and exploiting

cyberspace to enhance our defence – including the capability to exploit the weaknesses of our opponents.

Cyber capabilities may provide the kind of precise and tailored effects which a conventional attack cannot.

If, for example, we were able to switch off the lights for a window of opportunity, then this would provide decision makers with greater options.

However, we should not underestimate the investment required to develop such capabilities; the intelligence, understanding and overall resource may be significant.

It is also the case that cyber cannot put boots on the ground, dominate the sea lanes or control the air – all of which remain critical to preserving national security.

We still live in a physical world – so physical capabilities will never be replaced.

But they should be supplemented by cyber capabilities which will give protection where necessary and greater flexibility where required.

Defence Cyber Operations Group

As part of the SDSR, we are creating a new UK Defence Cyber Operations Group which will integrate our activities in both cyber and physical space.

The Group will provide a cadre of experts from across Defence to support our own and allied cyber operations, to secure our vital networks and guide the development of our cyber capabilities.

It will also be responsible for developing, testing and validating cyber techniques as a complement to traditional military capabilities.

There is much to learn and develop in this area.

It will take time to understand fully the threats and opportunities.

The Group will work closely with other government departments, industry and other experts.

International Action and the Law

Ladies and Gentlemen, there are no geographical barriers in cyberspace.

So our partnerships need to be international.

We will need to forge strong international alliances to increase resilience and joint operational capabilities.

As NATO is the cornerstone of the UK's Defence, so addressing cyber in the NATO context will be important.

Together with our NATO allies, we will need to establish a common understanding on how best to defend ourselves against cyber attack, and the role of NATO in our collective defence.

There is much discussion on the legal frameworks which apply to acts of aggression in cyberspace and those that apply during armed conflict itself.

I would argue that the established laws governing the use of force and the conduct of hostilities are equally applicable to cyberspace as they are to traditional domains.

When applying the law, one of the difficult issues will be determining if an event constitutes an armed attack.

For traditional domains, we assess the act, its effects, and the whole context to determine whether it constitutes a breach of international law.

We then judge what the necessary and proportionate response should be, applying well established legal principles.

Why should assessing and responding to a cyber attack be different?

Of course the issue of attribution in cyberspace will be difficult.

As will the issue of intent.

But as I said earlier, just because it will be difficult, doesn't mean it will be impossible

So I believe that the issues around NATO Article V may not be as difficult as some suggest.

But certainly Article IV and the recognition of threats beyond Alliance borders will be an important approach at this stage.

Conclusion

So in conclusion ladies and gentlemen when it comes to conflict, I believe we must recognise that actions in cyberspace should be governed by the same principles of international law which already act to check the worst extremes of state actions in the real world.

Under the last government, I believe too often, we sought to use international law to justify what had already been decided, rather than using international law to guide our decisions.

We need to have more respect than that.

We need to recognise how vulnerable Britain would be in a system of international anarchy.

We therefore, I believe, need to apply the principles of international law to cyberspace as well.

This may be difficult to achieve but the rule of law brings better security and better predictability.

It does not extinguish threats but it helps manage them, helps to define what is accepted and what is not.

This is what I believe is required if we are to protect the enhanced freedom of opportunity that the digital age can provide.