Former British SIS Agent Warns Public of Modern Cyber Terror Threat

Nigel Inkster is from the International Institute for Strategic Studies and has served in the British Secret Intelligence Service, focusing extensively on transnational issues, and eventually taking the post of Assistant Chief and Director for Operations and Intelligence. Nigel now serves the IISS in the role of Director of Transnational Threats and Political Risk. Here he outlines the current cyber security threat environment, definitions of cyber attack and cyber warfare, as well as future strategies for deterrence and interdiction. He also explores specific case studies such as the MI5 network security breach of 2009. This is an audio interview transcript.

Densmore: Hello and welcome to Defence IQ's Command Post interviews. Today we're privileged to welcome Nigel Inkster, Director of Transnational Threats and Political Risk, the International Institute for Strategic Studies here in London. Nigel, welcome.

Inkster: Good morning.

Densmore: Nigel, both cyber security and cyber warfare have been very hot topics lately – both in the UK and abroad. Can we begin by maybe giving an understanding of what the civil side of these issues are, compared with the military side?

Crystallising the threat picture

Inkster: Yes. This is one of those areas where it's very difficult to make clear distinctions between the civil and the military dimension in security terms. So many of the systems that we depend upon in our daily lives are now networked – dependent upon the functioning of the Internet, and any disruptions to the Internet can have pretty serious consequences, and of course, in a security context and in a military context, that's very significant.

I mean, I think we have to look at this as a spectrum with a full-blown warfare at one end of the spectrum – in which context, obviously, cyber warfare would simply become another component of warfare, and then going back down through what one might term cyber exploitation, which is, effectively, espionage and cyber crime, distinguishable only in terms of intent, because the techniques are the same, and then the kind of mischievous activity of hackers, independent groups, who are possibly working to create mischief for its own sake. So we have to think of it in terms of that spectrum, but of course, there are no clear dividing lines.

Densmore: And it sounds like there are… in what you describe, there are kind of four pillars of cyber activity on the, on the criminal side, going all the way up to cyber warfare. I mean, what might be, in your opinion, the notional idea of what cyber warfare might look like in the future?

Inkster: Yes. Okay. Well, I mean, again, I think we need to distinguish between full-blown warfare, where activity in cyber space is simply one more dimension of the battle space, and one might… cyber skirmishing, which I think is something that is going to carry on for the foreseeable future, and that is attempts by either a nation or a non-state group to access information and systems, either in order to obtain information or to manipulate the systems to their own advantage, and I think that sort of thing is… it's obviously going on all the time and will continue to do so, and there are some interesting questions around the extent to which that sort of activity can be regulated in… by some kind of international negotiation… international agreement.

I think it is important, because there is a case to be made for establishing some internationally agreed thresholds, beyond which activity ceases to become cyber skirmishing and actually constitutes an act of aggression, which invites some kind of retaliation. These are issues that have not really been addressed yet, but need to be. At the other end of the scale, if we look at what happened in Georgia in 2008, we saw that there was a cyber dimension to that conflict, as the government information and financial systems of the Georgian state were subject to disruptions at the same time that actual combat operations were taking place.

Densmore: So that would be the full scale cyber warfare that you're talking about, and that sounds relatively easy to… not easy, but maybe more definable than cyber skirmishing. In 2009, for our listeners, there was a security breach that took place in MI5's internal computer network, and there were… there was a bit of fallout after that, and I believe Lord West was the counter terrorism advisor at that time. That kind of cyber attack… would that be classified as cyber warfare, in your opinion?

Inkster: Well, I think it's important to set that in its correct context. The attack that took place was on the security service's website. In other words, its public face. In reality, of course, the corporate network of the security service will be air-gapped. It won't be connected to the Internet and all external media ports on computers in the organisation will be, will be blocked so that infected software cannot be introduced. It's pretty easy to attack a website of that kind – a public website.

Specific threats and appropriate response

It's not going to do the perpetrator any good in terms of seeking information about… sensitive information about the organisation or, you know, introducing infected software. So I think that is important… to get that in context. But of course, yes, obviously efforts will be going on all the time to look out and identify vulnerabilities. In the United States, for example, the Pentagon has highlighted a programme of attacks going by the codename of Titan Rain, which have focused on US defence and a variety of other US government websites.

It's not clear how much sensitive information was compromised, but of course, one has to think of it not just in terms of getting access to a particular set of sensitive information from one organisation, but gaining knowledge about the totality of how government works, and that carries a different set of vulnerabilities, but they're vulnerabilities nonetheless.

Densmore: And this raises the question too of appropriate response to the threat of cyber, of cyber criminal activity and cyber warfare activity, and you brought up the Pentagon's concerns about some of these things. For our listeners, the US Cyber Command has been established by the US military, almost as kind of an offensive operation to potentially… I mean, I imagine [unclear] in the future, some kind of cyber attack to a known threat. Do you see any kind of risk in this?

Inkster: I think there are potentially. I mean, it's important to remember that the head of the Pentagon Cyber Command is double-hatted. The person occupying the post is also the head of the NSA – General Keith Alexander – and of course, it is predominately NSA that will have the capabilities that are likely to be deployed in this context. Nonetheless, I think it is important for any country that is concerned about cyber security to engage in, shall we say, offensive operations, because that's really the only way that you can acquire an adequate level of situational awareness, which will enable you to appreciate and take measures against the threats that are out there.

So it is important to have some kind of… yes, offensive capability. Whether… and there has to be a military dimension to this. There has, I think, to come a point at which, if aggressive cyber activity amounts to, you know, an act of aggression in terms that would be recognised by the UN Security Council, the capability does exist to take appropriate and proportionate retaliatory action. Now, that, of course, is a whole area, which remains undefined and a lot more work and research and negotiation is needed to try and establish what that might be.

Densmore: And it sounds like probably in the UK, we know that that capability does exist, but it probably would take a different route, don't you think, than where the US has gone with this?

Inkster: Yes, it has done, because of course, up until now, the government's… the UK government's focus on cyber security has been directed through the Cabinet Office, which is, you know, in effect, the Prime Minister's department, through an organisation called the Office for Cyber Security, and that, of course, you know, very obviously doesn't have a military dimension to it.

There is, however, the beginnings of work within the British Defence Ministry to look at what capabilities they might need in the event of actual cyber warfare operations, and they're beginning to think about what those capabilities and organisational assets might need to consist of, but it's been done in a very different way, and with a focus, I would say, designed to be more across government – making sure that all departments of government understand their particular vulnerabilities and are alert to these and taking steps to minimise the risks.

Densmore: Which, again, sounds a bit on the education side? So educating sectors what potential risks are, as well as scaling up defensive measures across the board, as you said. Now, what could potentially be… and this, of course, may never happen, but worst-case scenario for a cyber warfare attack, can you paint a picture for us what that might look like?

Imagining full-blown cyber war

Inkster: Yes. I think it's very difficult to do that. I suspect it's going to be one of those things that we will only fully understand if and when it happens, but in the United States, some recent exercises were undertaken and… government exercises, and the results were, I think, pretty alarming, and the first point, of course, is the problem of attribution. You don't actually know, beyond any reasonable doubt, where these attacks are coming from, because their origins will be designed… be disguised.

Secondly, of course, your communication systems and all sorts of other systems on which you typically rely are going to disappear very quickly. Attacks are likely to focus on things like power supplies, financial systems, and one can imagine the confusion that would result if banking and financial systems were destroyed. I think the potential does exist in the worst case to do significant damage – obviously not on the same sort of scale as a nuclear attack, which is final and irrevocable, but I think significant damage could result.

Now, of course, it's not a once and for all situation, because as damage occurs, the potential does exist to restore systems that are affected, but all of this comes at a cost and involves significant periods of lack of communication, confusion… if it is linked with attacks on physical infrastructure, that could be yet more serious.

If, for example, one or more of the satellites that provide GPS signals that enable US precision-guided missiles to function are knocked out – either by simply nudging them out of orbit or by more drastic means – that obviously has a major disabling impact on the country's defence capabilities, but we would also suffer a potentially catastrophic loss of mobile telephone communications, with all sorts of knock on impacts, and I think the biggest thing about all of this is that none of these attacks are going to be confined to the military domain. All of them are going to have a significant impact on civilian populations.

Densmore: Which probably puts those attacks in the realm of terrorist attacks, I imagine, because that is, that is… the impact, it sounds like, affecting a civilian population. Do you have…?

Inkster: Well, I mean, I think if you look at the… what the laws of armed conflict say about this, deliberately attacking a military… a non-military target is, of course, a war crime under the laws of armed conflict, but how does one… where does… how does one draw the distinguishing line in a case like this? If the purpose of the attack is primarily military, but it has a secondary impact on a

civilian population - as is the case, for example, with aerial bombing of cities – then, under the laws of armed conflict, that is not deemed to be a war crime.

Densmore: And I think there are probably concerns too from our audience in preparedness, and we've done a couple of questions here and I'll jump right to those, since we're nearing the end of our time, but we discussed earlier and you talked about the need for the UK to do more work in terms of research and devising strategies for meeting some of these threats, and our first question addresses that. In relation to the Coalition's budget cuts, how might these affect UK cyber security in the future?

Inkster: Well, obviously they will have an impact, but these budget cuts are going to have an impact across the board. I think there is quite a lot that can still be done at relatively low cost in terms of public education, and also in terms of sending some important pricing signals to the private sector, because up until now, Internet security has really just not been an issue of concern to service providers or systems providers. The Internet was not conceived with security in mind, but security has come increasingly to the fore.

There is a lot that the private sector could do relatively easily and not that expensively to make the Internet a lot more secure than it currently is, but for that to happen, the private sector companies involved do need to get some clear steers from the government. So that's one thing that could be done at a relatively low cost. So I don't think… obviously, it will have an impact, but this not… this need not, in my view, inhibit governments from working to do more on cyber security.

Densmore: And certainly, the previous administration was keen to look at certain technological advances as defensive measures, and this gets into our second question posed by a reader. What is the potential use of biometrics, especially iris recognition, in the area of cyber security? Is it feasible and is it something we can put into play now or in the near future?

Inkster: Well, the honest answer is that I don't know about the technical applications of that on the Internet, but anything that helps to identify who is on the Internet to reduce the levels of anonymity, which currently exist, clearly, you know, is going to have benefit. At the moment, it's incredibly easy to hide on the Internet. Anything that reduces that risk is probably welcome.

Densmore: Nigel, thank you very much.

Inkster: Not at all. A pleasure.