NATO is coming to terms with the challenges represented by the cyber domain, according to Jamie Shea NATO's Deputy Assistant Secretary General charged with looking at emerging security challenges in the first of a new series of exclusive interviews of leading figures by Nick Watts for Defence Viewpoints.

Shea who has over 30 years' experience of working at NATO was recently involved in the working group which produced the Alliance's Strategic Concept. He has seen how the Alliance has transformed itself from a Cold War organization, through the campaigns in the Balkans and the admission of former Warsaw Pact members, to its present state.

Shea addressed the challenges which face a multinational organization as it comes to grips with the evasive and troubling threat in the cyber domain. He noted the widely publicized reports about how cyber crime was now larger than the narcotics trade. The fact that no lives have been lost so far as a result of cyber related attacks does not diminish the risk to the security of NATO Allies. "It is more than a nuisance" he said. The cyber domain poses a serious organizational problem as a cyber element is likely to be part of any future military campaign and NATO needs to respond.

The Alliance has begun to respond by establishing the Co-operative Cyber Defence Centre of Excellence (CCD COE) based in Tallinn. The working party, of which Shea was a member, drafted the Strategic Concept of November 2010 which recognized that "malicious cyber-attacks can reach a level that threatens national and Euro-Atlantic prosperity, security and stability." This was subsequently codified by a revised NATO Policy on Cyber Defence in June 2011 which emphasised the need for NATO to protect its own IT and communications architecture. Shea notes that NATO has over 100,000 computers and 30 significant communications networks.

Whereas previous security threats which the Alliance had to deal with were knowable and identifiable, such as tanks aircraft and missiles; the cyber threat is "unknown until it happens, and often not until sometime after it's happened." Similarly following the advent of nuclear weapons in 1945, it was not until the Cuban missile crisis of 1962 that international mechanisms were put into place to respond to the threat they posed. It might be that the onset of a crisis involving a cyber-attack will act as a catalyst to establish internationally accepted norms of behaviours between countries.

Shea says NATO recognizes that “cyber is different” whereas previously any IT related matter was referred to technical people, now top level military and political figures need to think about national and international rules of engagement and how to respond to attacks. This is as much about people and processes as it is about technicalities. Top level political buy in is needed to enable the technical matters to be addressed. With regard to NATO, Shea notes “we have got to learn to walk before we can run. To paraphrase Churchill; this is the end of the beginning.”

Concerning work in hand, Shea drew attention to what the Alliance was doing to test its own systems, and how it was helping applicant Member States to prepare themselves. NATO has established an incident response centre to up-grade digital forensics and to help with responses. A Memorandum of Understanding has been signed by 21 of the 28 Allies, to enable a rapid response team to assist with information sharing in the event of a cyber-attack. This information sharing process builds up confidence between allies and is helping to shape what might eventually emerge as a recognized standard of acceptable cyber security.

NATO now conducts an annual exercise, Cyber Coalition, which stress tests Allies’ cyber networks, as well as those of partners such as Austria, Finland and Sweden. Those Allies that are seen as more advanced in their cyber security preparedness, such as the UK and US are being encouraged to share information with those who are currently lass able. This will help to establish a good Information Assurance regime.

A further difference is the way in which NATO engages with industry. In other areas a requirement is identified and equipment is bought to meet it. In the cyber domain the nature of technological change is such that NATO will have to change its culture. In the new era a continuous dialogue with industry will have to replace the previous regime. “The private sector is key” notes Shea. A two way street based on information sharing will be needed. A NATO Industry Advisory Group study has examined this matter and the Alliance is currently looking at how best to carry forward its recommendations.

One by-product of this multilateral activity may well be to help advance progress in defining recognised standards of cyber security which at the moment is proving elusive. NATO’s process of codifying standards into Standard NATO Agreements or STANAGS may help. Shea is under no illusions that this will be easy, however, “NATO will have to become more nimble” he says reflecting the challenge that the cyber domain poses. Adaptability has kept NATO in business; the future looks full of tricky dilemmas which will call on all of the Alliance’s collective ingenuity. Managing the cyber threat may be a first step to dealing with others which may emerge.