NATO Information Assurance Symposium

NIAS 2012

Evolution, collaboration and innovation

NIAS 2012 saw a record number of thought leaders and decision makers from NATO and the technology sector converge at SHAPE, Belgium, to debate the evolving cyber-security landscape and the challenges and opportunities it presents in a rapidly changing world.

Attracting more than 1,000 delegates and 80 exhibitors from 28 NATO Nations and partner countries, NIAS 2012 cemented its reputation as both a highlight of the NATO calendar and as a leading information assurance (IA) event globally.

Offering a unique platform for networking, information sharing and collective problem solving among the IA and cyber defence community, the symposium – which ran from 11-13 September – hosted a premier line-up of speakers, technical workshops and vendors.

The launch of the NATO Communications and Information (NCI) Agency in July added another exciting dimension to a packed agenda, while facilities for delegates to question speakers live via Facebook, Twitter and SMS enabled a flow of ideas – aligning neatly with the symposium's focus on collaborative working and communities of interest.

NIAS 2012 got underway with an interview of NCI Agency General Manager (GM), MGen (rtd) Koen Gijsbers, by NATO's Deputy Assistant Secretary General for Emerging Security Challenges, Dr. Jamie Shea.

Setting the themes for the conference, the session explored the role, vision and priorities of the NCI Agency, the transition from protecting infrastructure to protecting information, technical and financial challenges, and the 'human factor' in securing data and information.

Evolution not revolution

Opening with a tribute to the NCI Agency's 4,000 staff, the GM highlighted the new agency's potential as a catalyst for change while emphasising that its role in providing effective and undisrupted support to military operations required its development be evolutionary not revolutionary.

"We are very motivated to develop an environment in which soldiers have the best tools available to do their work, but we are taking a step-by-step approach to ensure the Agency's operational support to missions is safeguarded on the one side, while bringing NATO into the 21st century on the other," he told delegates.

“The current environment is small pockets of very good IT, but collaboration remains a difficult issue as our systems were not designed with that in mind. We are now looking at NATO as an enterprise – the full body; operations, command structure, HQ, agencies and member nations – and seeking to optimise collaboration and IA in that environment.”

The GM said the NCI Agency was in a consolidation phase, adding: “The next step is to develop a new ‘engine room’ where all our technology and production is merged, using industry best practice. The third step is to innovate and modernise, which will deliver major improvements in our situation and the majority of savings.”

Threats without borders

The Agency’s genesis comes at a time of unprecedented change for NATO in the IA and cyber defence arena.

The increasingly sophisticated capabilities of its adversaries, along with an evolution in the nature, methods and motivation of security breaches, is driving a fundamental shift from the traditional focus on protecting information infrastructure to the security of the information itself.

The NATO Computer Incident Response Capability project has done much to define a secure infrastructure and strong perimeter, but the very concept is being overtaken by a world in which that perimeter is fluid, difficult to define and even more so to secure.

Meanwhile the introduction of numerous portable devices and multiple access methods, along with an ever-changing mix of suppliers, coalition and industry partners, is presenting challenges that were unimaginable just a few years ago.

“If you take military principles in your defence, what you want to do is defend in depth. It’s not good enough to just defend the perimeter, because if the enemy is already inside he can send the information outside – and he is doing that,” the GM warned.

Private sector partnerships

As cyberspace becomes ever more crowded, NATO needs technology that meets its specific requirements for multi-level security.

Soldiers in an operational environment, for example, urgently need greater bandwidth to support cryptology devices for secure transmissions. And in the absence of solutions, there’s a risk that users may find their own ways to get the job done – thereby increasing the potential for security infractions.

While NATO’s technical platforms are continuously improving, it’s seeking to adapt best-in-class solutions from industry and the private sector for its own requirements.

The GM told delegates: “There’s a lot of initiative in industry to develop solutions, but the problem from our perspective is that industry is not currently collaborating in ways that enable us to ‘plug and play’ into a system.

“We need solutions that can be pulled into the enterprise environment and work immediately without having to fix interoperability issues at a later stage.”

And he cautioned: “Any solution in the cyber arena is a snapshot based on the threat that we have at this moment. And that threat will develop and most likely increase, so we need to develop capabilities in a step-by-step approach.”

The human factor

As policy shifts from *need to know* to *need to share*, NATO is facing ‘human factor’ issues across the spectrum with lack of user awareness rather than technical issues posing the major risk.

The GM told NIAS 2012 delegates that the NCI Agency was looking at ways to improve the training of NATO personnel, explaining: “In an environment where we want to use the most modern technology it’s crucial that people are aware of the associated risks. If you give people mobile solutions they need to take ownership of the data on that device.

“In US airports last year more than 75,000 laptops were lost and only 30% were retrieved. So you can have security measures on the machines but ownership of information is an important element and it’s vital to what we do.”

In a world where NATO’s allies face attacks on both traditional fronts and from an invisible, often unpredictable threat in cyberspace, shared awareness is vital to defence.

A move towards more collaborative working with partner nations, the private sector and academia offers a unique opportunity to ensure capabilities are pooled, cost efficiencies increased and best practice is benchmarked more effectively.

Smarter working

An additional challenge for NATO is developing world class IA and cyber defence capabilities at a time of great pressure on defence budgets – a topic taken up during a separate panel discussion between NIAS 2012 Director, John Tatman, NIATC Head, Captain (USN) Navy Mike Thrall, and the NCI Agency’s Transition Director, Dag Wilhelmsen, Interim Deputy General Manager for Capability Development, Kevin Scheid, Interim Deputy General Manager for Service Provisioning, Rear Admiral Vittorio Di Cecco, and Interim Director of Operations, Brigadier General Guy Feat.

All agreed that organisational and infrastructure consolidation under the NCI Agency would drive efficiencies, as would smarter collaborative working.

“When the capabilities of several member nations need developing, we go to industry,” Mr Scheid explained. “Industry benefits and the nations save money. The NCI Agency is at the intersection of that and has the ability to infuse NATO standards and proliferate a common approach across the organisation.”

Mr Wilhelmsen added: “NATO members have agreed our goals for savings should be based on our operating costs, but that doesn’t include the investment in programmes we’re procuring. These will be made more cost-effective in future by reducing the time it takes to procure.”

Coming just weeks after the NCI Agency’s launch, NIAS 2012 provided a timely and prominent platform for the new Agency to showcase its vision for the future and to engage with potential partners in exploring world-class solutions to the tough security challenges ahead.

It also served to highlight the significant steps that have already been made in enhancing NATO’s IA and cyber defence capabilities, with the issue set to remain very much in the foreground at the highest levels of the organisation.

Authors: Emma Treadwell and Viv Morgan
Editor: Gus Mommers