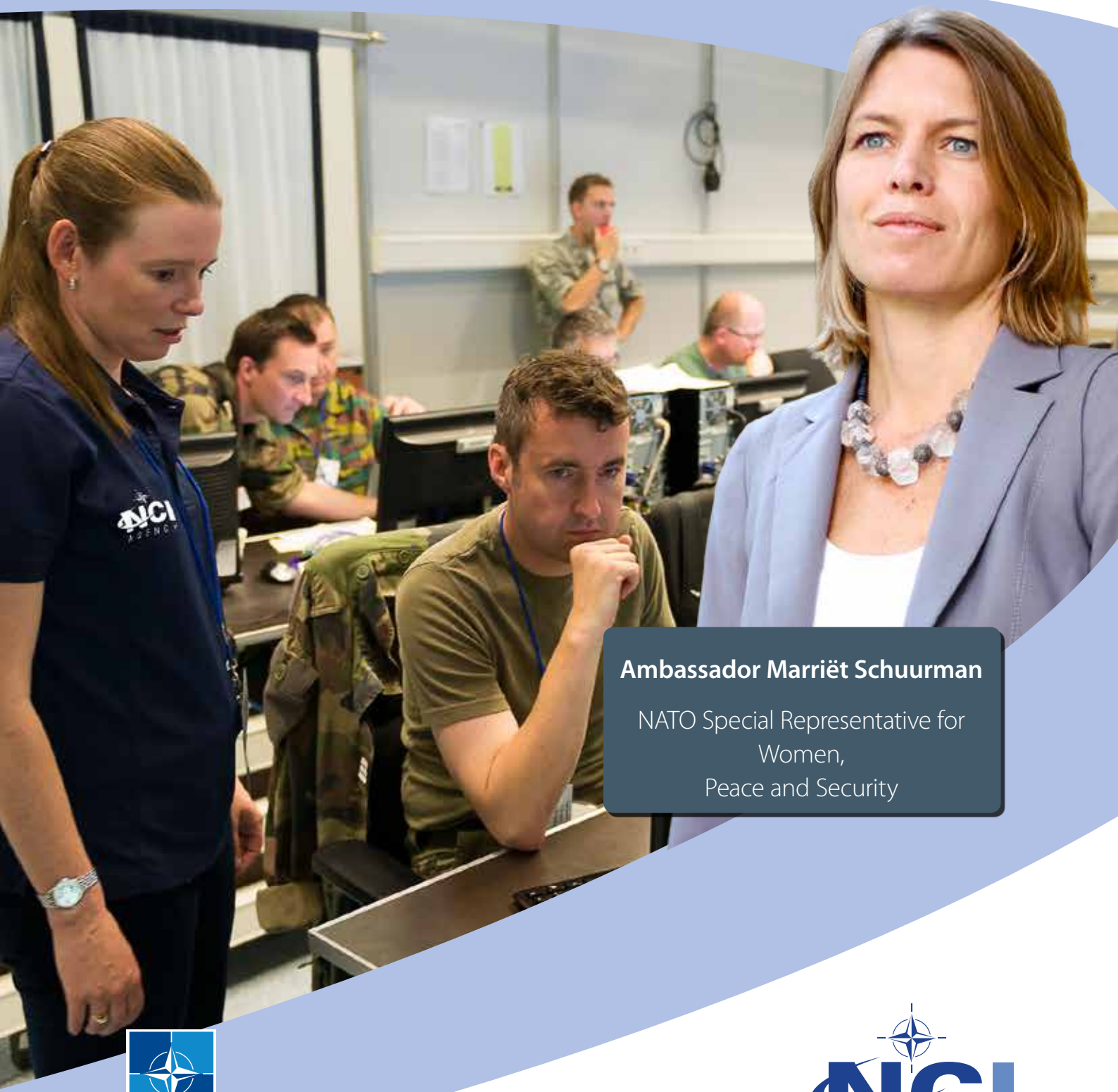
Communicator

Issue 3 | 2016



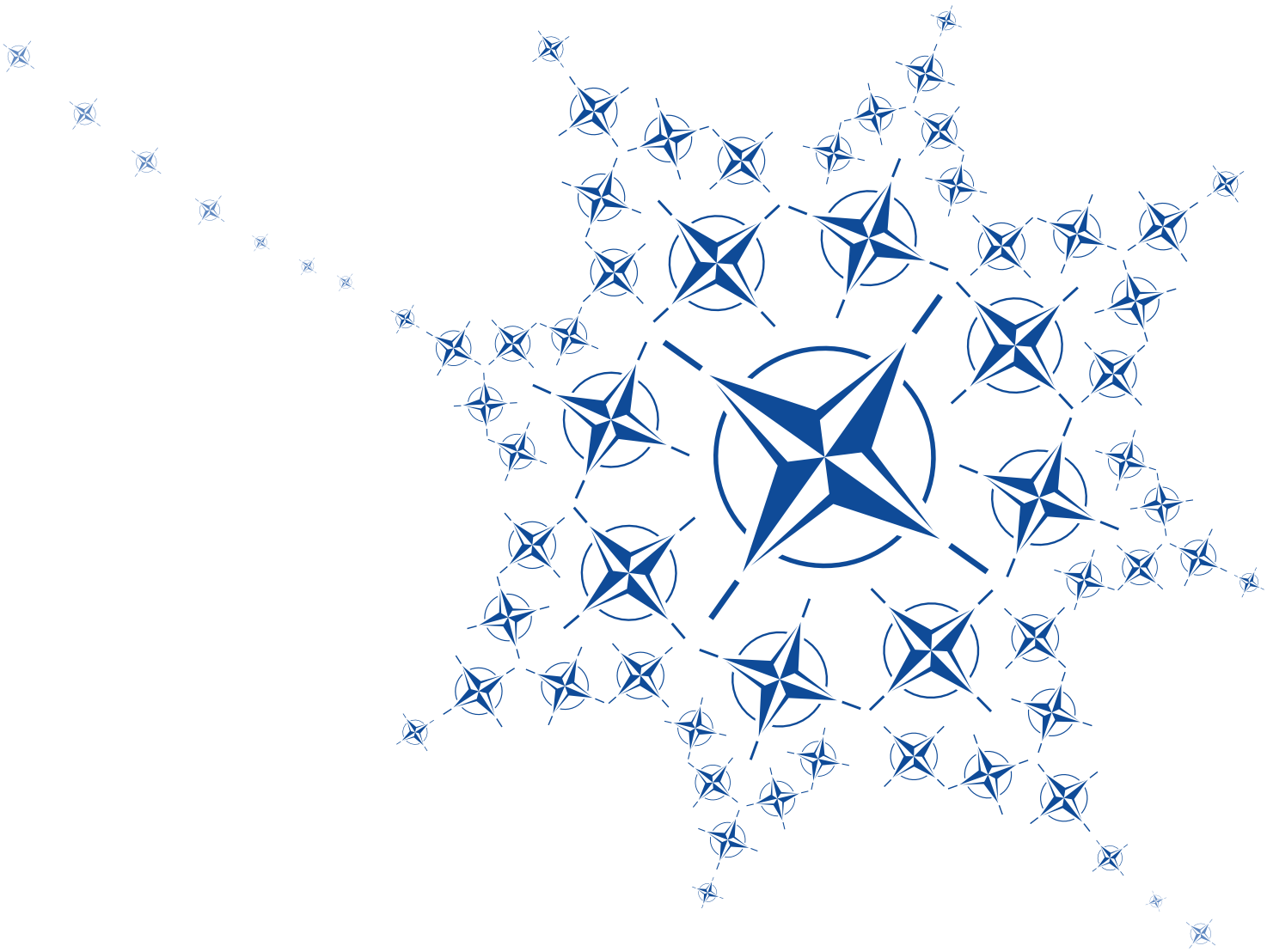
Ambassador Marriët Schuurman

NATO Special Representative for Women, Peace and Security

NATO OTAN

NCI AGENCY

Hacking, a way of life • ACCS - Protecting NATO's airspace • Triton, the messenger of the sea



NCI AGENCY

Season's greetings
and a Happy New Year

ISSUE 3
2016

Table of contents

12

Cover story: Ambassador Marriët Schuurman

06

Security at sea

18

LC2IS - Major step forward

30

What makes a great (cyber) leader?

If you are not a member of the NCI Agency, but would like to receive a printed version of our Communicator magazine, please let us know at: **communication@ncia.nato.int**

Chief editor
Michal Olejarnik
Editorial team
Adelina Campos de Carvalho, Lucie Cimoradska, Livia Jusztin-Majercsik
Layout
Andre van Herk / Dorena Timm
Print
NCI Agency - Creative Media Centre

360° agility

No rest for technology. No sooner had we celebrated the delivery of key capabilities for NATO's landmark Warsaw Summit, than another set of challenges loomed on the horizon.

What the team delivered for Warsaw was remarkable and has my deepest appreciation. To give just one example - new NATO headquarters in Eastern Europe were connected in record time. Meanwhile, software delivered by the Agency, in partnership with Industry, enabled NATO's missile defence shield to reach initial operational capability.

You would think a brief respite would be possible. Not really. NATO has just launched a new operation, Sea Guardian, to boost security in the central Mediterranean. And the Commander of MARCOM has an even more farsighted vision of how information technology should support his mission.

As our Presidents and Prime Ministers emphasized at the Warsaw Summit, the world is facing a new time of insecurity. For us – NATO's technology provider – this means a premium on agility, to always be ready for the next challenge. Part of that is relentless innovation as highlighted in our new Technology Watch section.

But the ultimate essential are our people. I am extremely proud of the fact that our cyber defenders have been recognized as one of the top three teams in the world by a leading cyber security magazine, and that Ian West, our Chief of Cyber Security, received the accolade of CSO/CISO of the Year.

In these complex times, the more diverse and creative a workforce is, the better it can answer the next challenge. Hence our cover story. I am pleased that with 16% of our staff being women in 2016, compared to 14.3% in 2014 and 15.5% in 2015, the Agency's gender balance is improving year-on-year. Diversity, be it age, gender or nationality is our strength.

If you are looking for calm and relaxing times, do not come to the Agency. But this world-class team is always on the lookout for new talent to help us better support NATO's missions. In a word of '360° instability' with security risks to the North, East and South, there will always be pressure. Today's spectacular success will all too quickly be eclipsed by tomorrow's challenges. But that is precisely what makes this work so rewarding – pretty much whatever NATO does, wherever it does it, depends on our support. That is a source of pride, but also a great responsibility. Enjoy the reading.

If you like the new and refreshed take on our magazine, then please join me in welcoming a new member of the editorial team, Adelina Campos de Carvalho. Feel free to reach out to her, and the rest of the team, with story ideas.

NCI Agency General Manager
Koen Gijsbers

SECURITY

at sea

NATO is facing some of the greatest security challenges in a generation, with a more assertive Russia, growing instability in the Middle East and North Africa, and a permanent terrorist threat from ISIL and others groups with multiple collateral effects.

Many aspects of these challenges involve activities at sea, and have once again placed maritime security high on NATO's agenda. This domain falls under the responsibility of the Headquarters Allied Maritime Command (HQ MARCOM), which is supported by the NCI Agency's CSU (CIS Support Unit) Northwood.

Vice Admiral Clive Johnstone CBE, Commander MARCOM, believes that the main threats we face today in the maritime domain are three-fold, and that the Alliance cannot face them without investing in better communications technology.

He counts among these threats Russia's aggressive posturing in the Mediterranean, Baltic and Black Seas, the deepening migration crisis, and terrorism perpetrated by the so-called Islamic State of Iraq and the Levant (ISIL)/Da'esh which has caused increased insecurity in the Mediterranean.

"The threats are starting to affect the Sea, and it's probably the last great domain where there is complete freedom of movement, where good guy and bad guy can both operate and therefore we must think about it," VADM Johnstone explained.

"And of course the Sea is not just the waters, it's what happens underneath, what happens above it and what happens in space – so we must think about how we are going to operate in that domain and that's my responsibility."

With such a large responsibility, it is essential for the Commander MARCOM, and through him the Supreme Allied Commander Europe (SACEUR), to be in contact with scores of ships from Allied Member Nations at any given time.

The NCI Agency is working with MARCOM to provide this critical capability.

Connecting national navies

VADM Johnstone explained NATO Nations have a large number of ships at sea at any one time, with sometimes as many as 160 Allied ships, across the whole of the NATO Area of Responsibility. Some of these ships are assigned to MARCOM, while others remain under national operational control.

"Now they're at different stages of readiness, some of them are doing very basic training and but with all the rest, that's still a hell of a fleet. Again it ranges from little tugs up to aircraft carriers, but just imagine, if we can give them using NCI Agency's technology, the same picture, if we have an ability to talk to them…

If I have an ability to talk to the fleet commanders at their desk, not in a corridor, [or on a] phone down the road, if we can share this information and picture as a conversation then I don't need a standing naval group of 10 ships or whatever."

VADM Johnstone noted the interconnectivity technology provided by the NCI Agency will eventually give him the flexibility to reach out to Member Nations and point to the same tactical picture. This will allow MARCOM to build on its maritime situational awareness in areas where Allied ships are already operating.

"They will be doing national tasking but they will also be doing NATO tasking. And that interoperability process gives us a double plus rather than the single plus that we have at the moment. So there is a real virtual benefit out of connecting people better and talking to people better.

We're not there yet… But we have a real route march to get there. The NCI Agency is fundamental in allowing me to do that because I need the picture and I need the communication systems."

Without this type of technology, the coordination and management of NATO maritime tasking remains much more difficult.

Building the bigger picture

Allied and Partner Nations share information, but there are limits to what they share based on legal restrictions and other complicating factors, explained VADM Johnstone.

Nations, businesses and other stakeholders interested in security may not be able to share all their information, but they may be able to share some of it, and this can add up to a better overall picture of daily activities at sea.

"So what I'm trying to do is build, with [the Agency's] help, data systems that allow them to share 5% of their national picture or 10% of their national picture. So little data, big difference.
By giving us that 5%-10% times 5 or times 6, we have 100% if not 200% better situational awareness than we would ever have normally.

And then that allows us to task other navies, the French, the Spanish, the Italians, the Brits, the Americans, to go and plug the holes for which we don't have the facility at the moment.
So rather than giving warning times or stuff like that, what the NCI Agency does is it allows us to change culture and change behavior."

Cooperating for safer Seas

Operation Sea Guardian, which was created at this year's Warsaw Summit, is an example of NATO's renewed focus on the maritime domain, with Allied Nations providing ships to conduct a number of maritime security operational tasks in the Mediterranean.
It succeeded Operation Active Endeavour which saw NATO ships patrolling the Mediterranean and monitoring shipping to help deter, defend, disrupt and protect against terrorist activity in the region.

Sea Guardian kicked off in November 2016 with three NATO ships and two submarines – the Italian frigate ITS Aviere, the Bulgarian frigate BGS Verni, the Turkish frigate TCG Gemlik, the Greek submarine HS Papanikolis and the Spanish submarine ESPS Mistral – conducting the first patrols in the central Mediterranean.

The Operation covers a broader range of tasks, and is currently providing support to maritime situational awareness and to counter-terrorism at sea, as well as contributing to maritime security capacity-building.

"I see Sea Guardian as almost Sea Guardian 1.0. We now need to build in Nations' confidence, get in more capability and technology – that's where NCI Agency comes in – so we can prove the value of what we are doing.

We need to show that there is a demand signal for a Sea Guardian 2.0 which will give more freedoms, more strengths, more everything, and allow us to operate in the Mediterranean."

VADM Johnstone believes that Sea Guardian could set a new standard for collaboration in the maritime domain which could then be applied to MARCOM's whole Area of Responsibility.
This would have the advantage of seeing the navies of Allied and Partner Nations "all talking the same language" and ready to assist when a situation arises.

This sort of interoperability would reinforce partnerships with the European Union, such as the recent cooperation between the EU's border management agency Frontex and NATO in the Aegean Sea.

"An example of where MARCOM and the NCI Agency worked together very well and moved with speed was when we were asked by the North Atlantic Council to go into the Aegean. Within 18 hours we deployed task groups into the Aegean, we moved them from other parts of the world to cover and we took some precautionary steps but the thing that limited us was our ability to talk to FRONTEX and the ability to talk to NGOs and whatever.

And the NCI Agency was very quick in supporting us with laptops that allowed us to talk to FRONTEX on their least restricted communication circuits and talk to the EU.
Now that worked really quickly, and because of the work that the Agency did and the work that my guys did here at MARCOM, we could have linked up with FRONTEX's most secure sites within days if not weeks."

By Adelina Campos de Carvalho, Creative Media Centre.

Unified Vision 2016

Building Alliance capability for future operational missions

NCI Agency has helped the Alliance prepare for future operational missions by providing crucial support at the Unified Vision 2016 trial.
An integrated Agency team, led by the Joint Intelligence, Surveillance and Reconnaissance Service Line, lent their technical expertise to the NATO event. Unified Vision (UV) trials take place biennially and test the interoperability of Joint Intelligence, Surveillance and Reconnaissance (JISR).

The NCI Agency team, which also included personnel from General Services, Command and Control (C2) and Integrated Verification and Validation Service Line, were praised by Colonel Michael Clark, Allied Command Transformation, for their outstanding teamwork and cooperation throughout the trial.

Trial Manager COL Michael Clark said: *"The subject matter expertise [provided by the NCI Agency] in JISR, and in C2, were crucial for us [Trial Management Team] as we crafted the exercise..."*

"Their technical prowess was essential in supporting the network, enabling the underlying transport layer between us and all of the PED [Processing, Exploitation and Dissemination] and collection capabilities."

Unified Vision took place at the Warrior Preparation Centre at Einsiedlerhof, Germany, in June 2016.

It was distributed across 10 locations, and included eight Intelligence, Surveillance and Reconnaissance (ISR) simulated sensor capabilities, four live ISR assets, 17 Nations, 380 workstations and more than 400 personnel.

The UV16 trial focused on improving the federation of Processing, Exploitation, and Dissemination of ISR information across National and NATO Commands.
It also assessed the interaction of JISR activity with Intelligence, Operations and Target planning in a joint environment.

The work conducted throughout the event, will contribute to the delivery of NATO Alliance Ground Surveillance (AGS).

This will greatly improve the intelligence picture Commanders receive on the situation on the ground.

It will also help increase the wider integration of NATO Airborne Early Warning and Control (NAEW&C), which provides an airborne surveillance, warning and control capability that is multinational and immediately accessible.

It is clear that the benefits realized from UV16 will have a positive and constructive impact on the future effectiveness of JISR within the Alliance.

The NCI Agency team took on a number of key responsibilities during the event.

The team notably built operational vignettes which are simulated scenarios of military operations used during the trial to provide specific role-play for designated actors and response cells.

Although the core data produced during UV16 was simulated, there was also a small live-flying component.

This activity occurred within national borders and aided the testing of various capabilities including Full Motion Video (FMV) and Electro-Optical/Infra-Red (EO/IR) Imaging.

Meanwhile, NCI Agency experts also connected nodes via the Combined Federated Battle Laboratories Network (CFBLNet). CFBLNET allowed PED nodes to achieve connectivity within a short timeframe and with ease, which was recognized by participants outside the Agency.

The team was responsible as well for providing support throughout the entire UV16 life cycle. This included CIS aspects combined with operational expertise.

Agency subject matter experts in JISR, Intelligence Operations, Electronic Warfare and Command and Control were critical to the development of trial scenarios.

The team also helped oversee Tactics, Techniques and Procedures trialled and tested in UV16 and ensured they were effectively incorporated - technically as well as operationally.

By Laryssa Patten and Bob Essad,
Joint Intelligence, Surveillance and Reconnaissance.

Unified Vision 2018

With the successful completion of Unified Vision 2016, NATO has already begun planning the next edition of their Joint Intelligence, Surveillance and Reconnaissance (Joint ISR) Exercise series.

Unified Vision 2018 (UV18) is expected to be held across Europe and North America, further testing the concept of a global Federated Processing, Exploitation and Dissemination (PED) enterprise.

Dr Richard Wittstruck, Senior Advisor to NATO's Joint ISR Capability Area Manager and former chairman of the Joint Capability Group for ISR, has explained why Federated PED is so critical to NATO operations.

"Now in the pace of digital warfare, some targets are a matter of seconds and then they are fleeting.

So you have to be able to prosecute that target in a matter of minutes not hours, and that's what part of this federated PED has been about.

It's how quickly can one take in a collection against the target, process it, exploit it and then disseminate it back out to the network for decision and effect.

So we will probably spend more time focusing on the temporal variable [in future editions of Unified Vision].

We are looking at how quickly you can do something like reconnaissance and surveillance versus time-critical or time-sensitive targeting."

Dr Wittstruck discussed the evolution of the Unified Vision trials and what we might expect from UV18 as it builds on the lessons learned from previous exercises.

"What we learned in UV14 was that we had distributed PED in several sites throughout Europe and North America, but we did not have a doctrine that administered this process of managing PED sites across national and geographic boundaries.

So we took the good work of UV14 and we decided in UV16 to expand our role with Command and Control of Joint ISR by focusing on time-critical and time-sensitive targeting.

What made UV16 distinctly different from its predecessors is that there was a lot of simulation and virtual injects, and no Host Nation.

UV18 will probably leverage onto this experience and look to where we want to go next in terms of doctrinal development and technical operability.

We will also look at force protection because that's one of our key mission threads in NATO is force protection."

NATO'S CYBER DEFENDERS

Hacking, a way of life

Roberto Suggi Liverani was just five years old when he started playing with computers. He learned how to pick computers apart, how to code, and what began as child's play soon changed into a vocation. Making the jump to working in cyber security came naturally.

Hacking is often seen as a danger to governments even to society, capable of causing chaos as we rely increasingly on digital data for our daily lives. But there are ethical hackers, and many of them work alongside organizations and companies constantly testing their defences to ensure that they are resilient enough to face cyber attacks.

Roberto has been a professional ethical hacker for over a decade and most recently for the NCI Agency, protecting NATO's networks and applications.

"People like us who hack professionally are called white hats, to indicate that our work is to secure networks," Roberto explained.

"There are different groups. There are people working underground as black hats, there are people who are in between, 'grey hats' - sometimes they work with organizations or companies, sometimes they don't.

Each of us at the Agency has a different background. In my case, it's a passion that has always been with me. And I taught myself many of the skills which I now use every day.

In this field, experience and learning by doing is key, while academia does not always mirror the quick evolution of this industry. So after obtaining a scientific diploma, I began working as consultant. I was doing penetration testing for various customers in different industries, such as finance, banking, insurance and telecommunication, before joining NATO."

International team and unique skillset

The Agency's Cyber Security Capability Development team is based in the Supreme Headquarters Allied Command Europe (SHAPE) in Mons, Belgium, and The Hague, Netherlands. Cyber Security testing, validation and configuration is conducted from Mons, while Cyber Security innovation, planning and design takes place in the Hague.

Roberto works as a Senior Security Engineer for the Cyber Capability Validation cell based in Mons, which is made up of world-class security experts.

"This is the team to be if you never want to stop learning, hack and break stuff professionally. We have excellent people, like Vincent Hutsebaut, who came first in international CTF [Capture the Flag] hacking challenges - these are global challenges played by people all around in the world. If you score high points, it means you are very talented."

The Italian national and his talented colleagues are experts in both offensive and defensive security, web application security, cyber defence exercises, network security and forensics. All of them also have a deep understanding of how malicious hackers operate.

Part of their work involves penetration testing, that is to say looking for weaknesses in systems and reverse-engineering, which is a technique to hack into a software so as to understand how it works.

The cell also tests NATO networks by red teaming - simulating cyber-attacks from adversaries during exercises.

Continuous security testing

With over 400 million cyber events processed by NATO Security Sensors daily in 2016, it's no surprise that our cyber defences need to be constantly checked and made stronger.

A critical part of cyber security is to understand whether both in-service systems and systems under development are appropriately protected. Improvements can be implemented before a vulnerability is exploited, by assessing the strength of security mechanisms,

"What we do every day is we test everything before it gets deployed into NATO networks like software, everything that is used by NATO communities or NATO entities," Roberto said.

"And every day, we find vulnerabilities. Some days we find some that no one else has found before – we call those 'zero days'.

And we work with vendors like Microsoft, Oracle, McAfee, TrendMicro, IBM and others, providing them these vulnerabilities so they can patch them.

It's necessary to have this team and exceptional skillset in-house. It's part of the lifecycle of software.

As we speak, my two colleagues Diego Gianni and Francois-Xavier Stellamans have found vulnerabilities in two mainstream software products.

We are very busy, we are so booked with tests that if you were to ask us today to test something, it would take place in [three or four months' time] because we are fully engaged."

This critical work brings the cell in contact with many authorities and entities across NATO and Member Nations.

"The internet is a jungle"

Roberto and his colleagues have a unique understanding of the threats NATO faces and their possible disastrous consequences. Given the unique nature of NATO's business, the failure or the compromise of a critical system could possibly jeopardize a mission and endanger the lives of civilians and soldiers.

"[A hacker] can break the system, can make something not work… They can make it so that no one else can connect to a website, or they can get into the website, change content, compromise the database and steal information," he revealed.

"We work on testing very sensitive, very critical systems, like Air Command Control systems.

We have to have a certain level of clearance to do this type of work.

We have to make sure that these systems cannot be attacked easily or cannot go down in theatre or during a mission. They have to remain available.

What we do is all defensive so we try to find vulnerabilities and help the developers fix them to make our software and products more secure and robust".

"The internet is like a jungle," he added. *"Every day, every moment, there are always entities coming, new malicious hackers trying to get through, trying to get in.*

There is no face to the cyber attacker, you can be located anywhere, and in some countries you don't have any legal liability, so basically to me, we are always under attack."

Hacker Community

The Agency's cyber defenders are all active members of the wider cyber security community so their skills remain up to date and relevant.

"My colleagues and I are involved in the [cyber security] community. The community is a great way to exchange information techniques, discuss vulnerabilities.

I presented at security conferences, like DEFCON, EUSecWest and Hack In The Box, where we exchange tips and tricks, produce security research.

We publish articles from time to time, we also publish details of testing techniques, release scripts and tools.

For instance, my colleague Filip Waeytens, one of the founders of Brucon [Hacking Security Conference in Belgium], has contributed to BackTrack, which is a collection of tools for hackers.

We are heavily involved in research. And when possible, we try to attend major security conferences where you can find fellow hackers."

By Adelina Campos de Carvalho, Creative Media Centre.

Special Representative for Women, Peace and Security

Ambassador Marriët Schuurman

NATO has had a Special Representative for Women, Peace and Security since 2012. Ambassador Marriët Schuurman is the second woman in NATO's history to hold the prestigious position. She took up the position in 2014 and has been working tirelessly since to promote greater gender balance within NATO. Ambassador Schuurman's office, where we held this interview, is bright and cosy with comfortable armchairs. When we met her she looked fresh and trendy, and welcomed us with a big smile on her face.

How did you become the Special Representative for Women, Peace and Security to the Secretary General?

Pretty much the same way anybody gets a position at NATO. I went through the same recruitment process like anybody else, after being asked by the Dutch Minister of Foreign Affairs whether I was interested in applying. I was announced as a Special Representative by then Secretary General Anders Fogh Rasmussen as one of his last acts in office during the 2014 Wales Summit.

I'm sure it took quite a competition to get there. What do you think made you the right 'man' for the job?

They asked me at the interview what the measure of my success would be. I said, if I made myself redundant by the end of my term, I would be really successful. To be successful in acting as a reminder to policies, promoting diversity and integrating gender perspectives a lot of changing of mindsets is required, it does not happen overnight. So, I have to say, three years are not enough to make myself redundant. But, what I would like to see is that gender-awareness is a normality and is seen as a marker of professionalism for everybody who works here.

When people hear NATO, most of them instantly think of armed forces and operations. Military is still a profession, which in most of the countries is a dominantly masculine trade. How are women represented in the Alliance's armed forces?

We have been receiving national reports about women in the armed forces since 2000. The NATO Committee of Gender Perspectives is a committee which includes representatives of all Allies, as well as representatives of partner countries and focuses on balanced workforce in the national armed forces. We constantly urge national contributions to missions to send mixed teams, to have mixed troops, and to pay special attention to gender-balance in groups when interacting with locals.

Do you have specific figures?

Among the Allies there is an average of 10.3% represented by females in the national militaries, while 5.6% are deployed in NATO-led operations. Even though this rate is really low, the United Nations (UN), which it the most alike international organization to NATO has never managed to raise it above 4%, either. In order to improve this, we keep sharing best practices with the UN and regularly discuss our strategies on gender-balance.

How about NATO civilians?

Since 2000, there has been an increase of the number of women holding decision-making positions in NATO, but for three years now this number has been stagnating. We constantly need to seek for the best and the brightest, and if our finds are not balanced, it is not because the pool is not balanced. It is because we lack the effort to look further.

Where do you see your role in changing this at NATO?

I'm trying to be a platform, travel a lot and present best practices. There are great events raising awareness on women in uniform all over the world, be those video recruitment campaigns or a photo exhibition. It is really interesting to bring these initiatives together, to learn from them and share them in NATO.

Does such a unique international military setting as NATO come with an elevated number of harassment reports?

I don't have statistics on reported harassment, but I know there haven't been a single one report in the last year. Now, not having any complaints usually means that your complaint mechanism is not working. Harassment on the scale from bullying to sexual harassment happens everywhere.

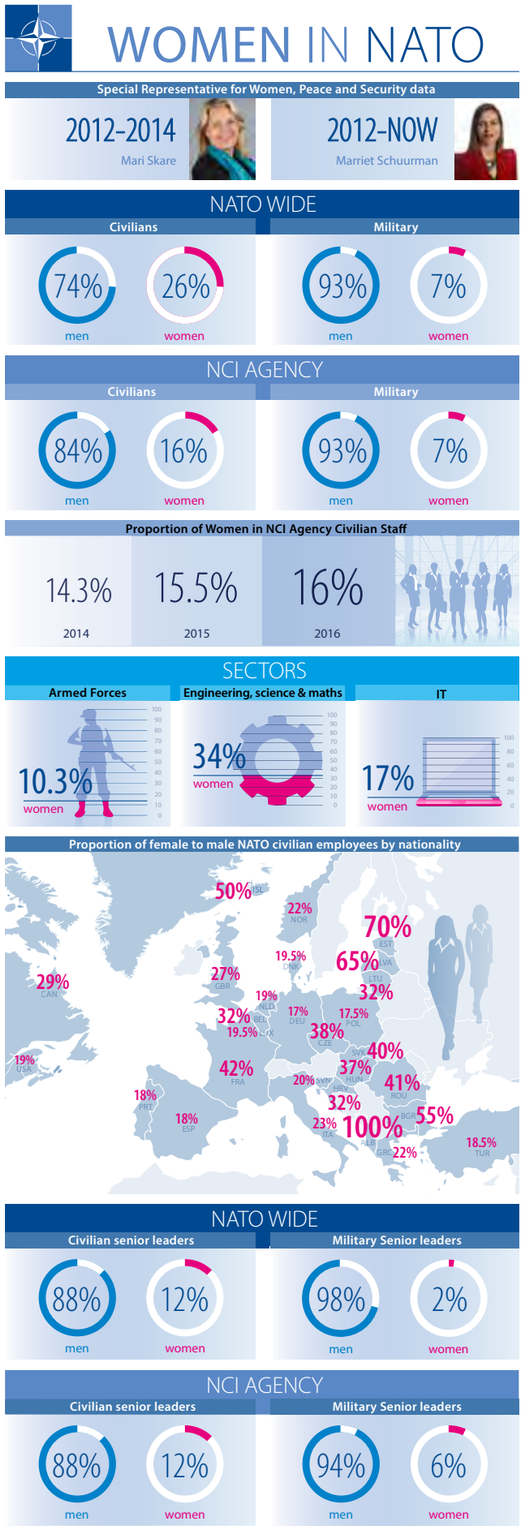
Do you know of plans to enhance the policy, to make it more visible, more precise?

NATO HQ is working on a new version of both the 'Prevention and management of harassment, discrimination and bullying at the workplace' policy and the code of conduct to make them more visible and to let everyone know about the 'what to do if'. The major problem with the existing documents is that they don't specify what you have to do or who you should contact if you witness or suffer harassment. They don't guarantee securities and don't explain the 'report investigation consequence' procedure. We are contributing to a Human Resources' project of updating the current harassment policy with our insights and experience.

If a woman would like to build a career at the NCI Agency, she would not only have to tackle the military quality of the organization, but most likely work in the field of technology, which is in 70% dominated by males world-wide. What would you tell those who would like to make it in the IT sector?

The number of female graduates in science and engineering in the Allied countries is shockingly low (34%)[1], so it starts with convincing

1 Eurostat, 2014



girls to carry on their studies in the field of Information Technology.

The increase of female graduates, however, won't automatically mean that your organization will employ more women. There still are many invisible and visible barriers. Not only young women but young men also get discouraged, when they see a long, bureaucratic job description phrased and structured very much out of their world, basically an invite to an old men's club. If we want to have the best and the brightest, we need to speak their language and need to take their preferences into consideration. They want to work in a dynamic environment, which is flexible and allows them to cater other priorities of their lives.

What can I as a staff member do to raise awareness on potential imbalances?

First of all, prove to everyone around you that you indeed are the best choice. Do your job as good as you can, make yourself recognized by what you do and happily ignore prejudice.

Don't let anyone get under your skin, don't let them affect your decisions. Just prove prejudice wrong.

Do you see NATO starting to welcome this approach? Are we soon ready to challenge Google in terms of recruitment policies and working environment, applauding individuality and promoting alternative working means?

We want to be an A-label on the job market. Obviously, it's hard to compare NATO to a business like Google, but when we look at our benchmark international organizations like the EU or the UN, yes, we definitely want to be the most attractive, most modern and most advanced among all of those. Unlike any business, though, we not only have to appeal to potential candidates, but also to the people who gave us mandate to operate, the Nations. We need to stay trustworthy to them. NATO has never been as necessary as it is today, and we need to use our networks, also the informal ones, through young people to make sure this message is delivered. I don't think there has been a better time to work at NATO than today.

How can traditionally rather bureaucratic NATO stay relevant in such a rapidly changing environment?

We need to change rapidly and to adjust constantly, too. Changing the organization means changing the mindset. Our recently started change in organizational culture programme also serves this purpose.

What would you say a good example is in this programme?

One example, changing the mentality from 'sitting on knowledge' to 'sharing knowledge', or going even further: creating knowledge. In order to achieve this, we not only need teams of creative people, but mixed teams in terms of gender, age and culture.

By Livia Jusztin-Majercsik and Nadja Elfertasi, Chief Strategy Office.

TECHNOLOGY WATCH

We won't experience 100 years of progress in the 21st century – it will be more like 20,000 years of progress (at today's rate)[1].

Welcome to the first instalment of Technology Watch. With each new issue of the Communicator, Technology Watch will give us the opportunity to share with you one or more emerging technologies that we believe will be important to our business in the coming three to five years. It is our intent to provide more visibility to technology, and more importantly, to understand how it may affect NATO's business.

Technology may impact business because it presents opportunities to deliver new or improved services to NATO users, or because it is something that can be exploited by NATO's potential adversaries to our disadvantage. We have intentionally decided to focus on the three-to-five year horizon so that the information we provide is timely enough that it will allow us to react and prepare, but not so far in the future as to be irrelevant.

We begin this first instalment with a discussion on the very general topic of the pace of technological progress, as we see this increasingly rapid pace as both a threat and an opportunity. In later issues, we will look at technologies such as: cognitive computing, the Internet of Things, quantum technologies (encryption, computing, and sensors), convergence in end-user computing, automation and robotics, the end of Moore's law, additive manufacturing, etc.

We hope that you will find the Technology Watch series an interesting read and useful to your work.

1. Ray Kurzweil, The Law of Accelerating Returns, 7 March 2001, http:/ www.kurzweilai.net/the-law-of-accelerating-returns

Technological Velocity

The pace of technology advancement has never been greater in the history of humanity than now, and there is no indication of it slowing down; in fact it is speeding up. This acceleration has been fuelled by the shift of innovation driven primarily by government, such as Defence or space research and development, to innovation driven by industry. While it was the US Defense Advanced Research Projects Agency (DARPA) which invented the internet, it has been the thousands or millions of corporate entities of all sizes that have evolved and proliferated this technology and exploited it for uses unimagined a few years ago. Niche defence technologies that cost millions of Euros a few years ago are now commodities in the commercial market, with market forces driving prices down, putting them within reach of a large part of the planet's population – including our adversaries.

Drones with capabilities that were strictly the purview of the military, are now available for a price that puts them in the hands of aficionados. Smart buildings are constantly improving their efficiency, monitoring conditions and resource usage, and ensuring that heating, lighting and other systems are all optimized. Even street bins are monitoring their own state and signalling when they need to be emptied, thus reducing the need for wasteful visits when they are only half full. This also ensures that they do not overflow. Cognitive computing systems routinely beat human opponents at chess. Recently, a Google AI system beat a top-ranked human player in the highly complex Chinese game of Go.

Intelligent agents like 'Amelia' are replacing traditional call centres in a variety of situations. Big Data analytics allow data to be continually mined and connections found that would have been impossible to detect in the past. A hotel in Japan is mainly staffed by robots, reducing payroll costs by 75%.

In August 2016, China launched a satellite purported to be capable of generating and distributing encryption keys using quantum techniques. Cars are driving themselves on roads and space tourism is being aggressively pursued. We have passed the point where we have more devices connected to the internet than there are people on the planet. Where approximately 3.9 billion connected things were in use in 2014, this figure is expected to rise to between 21 and 50 billion by 2020[2]. The amount of data which will be produced by these devices, and will need to be analyzed and stored, is staggering. The security challenges are formidable.

What has changed is that we, in the Defence world, are not only no longer leading in these areas, in many cases, are not even keeping up. Consider the following [perhaps trivial] example that illustrates the issue. In 2007, Apple introduced the iPhone which was immediately available to the world, including our adversaries. Our regulations and risk averseness meant it took considerably longer, and indeed, a number of generations of hardware and software, before we could offer it as a service on our networks. We thus lagged in this capability by over five years as compared to our potential adversaries.

In our business, it will be imperative that we do not stand still and that all of us stay apprised of these evolutions, constantly looking for creative ways of applying them to benefit and identify our vulnerabilities where these technologies can be used against us.

> **!** Never before has digital technology been as cheap and widely available as it is today. Consequently, the number of people and start-ups trying to challenge the establishment has never been greater. The odds are no longer in favour of staying the course[3].

Future technical innovation in our business will be less about creating new things, and more about recognizing new things developed elsewhere, and exploiting these in creative and novel ways to the advantage of our users. All of us need to be constantly learning and keeping our eyes open to the outside, marrying up external solutions to internal problems, and ensuring that we harness the best ideas into our environment as rapidly as we can.

This goes beyond technical innovation. We need to learn from others' innovations in areas such as business best practice, finance, HR, procurement, etc. Innovation is not limited to what we do; we can also innovate how we do things. Innovation is a common responsibility shared by all of us in the NCI Agency, whether in a technical area or in a support area.

Our behaviour needs to recognize the pace at which our work environment is evolving. We must adopt methodologies that are agile in all of our activities. We need to shed practices such as fully analyzing every detail of a problem at the outset, at the cost of delaying decisions and not making progress at pace. Detailed analysis in a rapidly changing and unpredictable environment is unlikely to stay valid for very long, and thus unlikely to lead to solutions that are useful when delivered. Small frequent steps allow us to react to change before the next step starts and are more likely to succeed and remain relevant. Agile approaches also allow us to recognize failure early on, when the cost is still contained.

> **!** Our greatest glory is not in never falling, but in rising every time we fall[4].

All progress involves an element of risk. We need to create a culture where risk is not only tolerated but recognized and even celebrated. Of course, this needs to be balanced against the reality that defence and NATO are, and will remain, fundamentally conservative environments. Nevertheless, in order to stay relevant, we need to balance our inherent and well-placed conservativeness with a healthy appetite for risk. The world is changing, our adversaries are more diverse, and not all of them follow a conservative line when it comes to acquisition and use of technology. How we accept risk will define our ability to adapt, progress and remain a relevant partner to our users. Failing is a prerequisite to learning and advancing. Standing still is simply not an option; the bad guys will not stand still and wait for us to catch up.

By Peter Lenk, Service Strategy.

***Next time:** Cognitive Computing*

2. Tully, Jim, 'Mass Adoption of the Internet of Things Will Create New Opportunities and Challenges for Enterprises', Gartner, 27 February 2015, G00274959 predicts the 21 billion figure. Other estimates, for example from Cisco, predict that the number will be closer to 50 billion – S. Collies, "The Emerging Enernet: Convergence of the Smart Grid with the Internet of Things," Rural Electric Power Conference 2015, IEEE.
3. 'The Discipline of Market Challengers: Win in the Digital Age by Challenging the Status Quo,' 2015 Report No. 11, Gartner G00294900
4. Attributed to Confucius

Major step forward for the NATO

Land Command and Control Information Service

The NATO Land Command and Control Information Service (LC2IS) is the main functional service in NATO supporting land-heavy operations. In 2016, its operational implementation and planning both made significant progress.

The First German-Netherland Corps (1GNC) and the Rapid Reaction Corps France (RRC-FRA) are now very close to their LC2IS Final Operational Capability.

LC2IS provides a rich set of functionality, enabling the effective Command and Control (C2) of NATO Land Forces, supporting improved Situational Awareness and decision-making of the Land Component Command (LCC). LC2IS also enhances interoperability and collaboration within the Land Community of Interest, the Headquarters, and across the NATO-National Command chain. It provides a critical link for C2 and Situational Awareness between the NATO Command Structure (NCS) and the NATO Force Structure (NFS). LC2IS is also a key enabler of the NATO-wide Common Operation Picture as it provides an efficient tool supporting the production and management of the Recognized Ground Picture.

The LC2IS Increment 1.1 was successfully completed and implemented in the NCS following Final System Acceptance and Joint Formal Acceptance Inspection in 2015.

Meanwhile, the implementation and employment in the NFS progressed significantly in 2016.

Regular training

LC2IS is currently used in exercises that are scheduled annually according to a well-defined plan.

The main NCS Command supported by LC2IS (LANDCOM) – which did not have any major exercise in 2015 and 2016 - is now refining and implementing the operating procedures in preparation of the forthcoming exercises. Allied Command Operations (ACO) has recommended to employ LC2IS within the NATO Command Structure on a more regular basis in order to maintain the required set of skills.

With respect to 1GNC and RRC-FRA, the majority of Headquarters staff has been trained and will be using LC2IS in order to support their role as LCC or as Joint Task Force (JTF) in NATO led-operations. LC2IS is planned to be used in these Commands on regular basis throughout the year.

Operational implementation

LC2IS support for Crisis Response Operations (Kosovo Force) was requested by ACO in 2015.
The NCI Agency prepared an implementation proposal (Type "B" Cost Estimate) which was authorized and is now being implemented with Initial Operational Capability expected by mid-2017. LC2IS is intended to be used as the main C2 and Situational Awareness tool for the Kosovo Force, connected and fed by the Kosovo Force Tracking System (KFTS).

Roadmap for LC2IS evolution

In parallel to the operational implementation and the Operation and Maintenance (O&M) of LC2IS Increment 1.1, the roadmap for the evolution of LC2IS has made significant progress. The Agency submitted in July the authorization request for the evolution of LC2IS in the next five (Type "B" Cost Estimate for LC2IS Increment 2). Unfortunately, operational demand for the next increment significantly outstrips its planned budget.

The Strategic Commands are currently in the process of reassessing their minimum requirements before the Type "B" Cost Estimate can be revised and eventually authorized.

The evolution will likely include a first phase (LC2IS Increment 2) comprising a Mid-Life Update (MLU) of LC2IS Increment 1.1 by 2018. This increment will include a technology refresh and a significant interoperability enhancement. The objective of the second phase (LC2IS Increment 3) is a major overall enhancement of the functionality, interoperability and technology by 2022, addressing also the main lessons learned on the current capability.

Other NFS Commands have expressed their interest in the LC2IS MLU to complement or replace National capabilities.
Additionally, most NFS Commands have been involved in the specification of Increment 2 and 3 over the last years and are interested in obtaining this capability when delivered.

This trend points to the likelihood of seeing in the next five to ten years, LC2IS widely employed in both the NCS and in the NFS. This is expected to result in a major enhancement of the technical and operational interoperability of NCS and NFS, together with a significant cost saving as a result of the adoption of a common software product and shared services.

By Roberto Porta,
Land Command and Control Service.

INTERNATIONAL CYBER SECURITY SUMMER SCHOOL

Over 60 students took part in the second edition of the International Cyber Security Summer School (ICSSS). Graduates of 24 different nationalities travelled to the Netherlands to attend the well-subscribed course, which took place between 21 and 26 August 2016. The summer school was held in The Hague and organized by the NCI Agency, Europol, and The Hague Security.

Taking place at The Hague Security Delta campus, the course helped prepare young professionals for the challenges of cyber security in international organizations.
This year, organizers had the chance to welcome the NATO Cooperative Cyber Defence Centre of Excellence to support the event.

The week-long course focused on introducing students to technology, policy and legal issues, and to the concept of an integral approach being the long-term solution to cyber security.
"We wanted the students to understand why cyber security is a complex challenge, to see the connections between technology, policy and legal - essentially, to see the big picture.
We saw the future leaders and professionals of cyber security taking this approach back to their nations and organizations", said Michael Street, the NCI Agency's Innovation Manager.

Students taking part in the summer school were all young professionals, between the age of 25 and 30, just before or after their university graduation.
They were asked to submit a resume, a motivational letter and define their field of interest in cyber security as part of the thorough application process.

A total of 61 students out of 140 applicants were selected to take part in the course, which offered them an opportunity to network among other skilled graduates from all around the Alliance.

Michael Reiner, a student explained how the school widened his perspective on collaboration in cyber security.
"In the cyber domain, there is little agreement on terminology. Often, identical terms are understood to mean different things by various nations and organizations," he said. *"So, the heterogeneous composition of the International Cyber Security Summer School contributed to expanding our international perspective on shared cyber security concerns. This initial approach reflected the critical need for diversity in successfully countering the rising and continually-evolving cyber threat landscape."* The school included different activities, from presentations to networking events, as well as practical, real-life problem-solving modules.
Participating students demonstrated their talent by developing projects, which were in many cases relevant to the NCI Agency's and Europol's respective missions, and which may be further developed in the future.

The innovative approach and views of these young cyber security professionals gave the organizers a fresh perspective on several challenges they face in their daily work.
The highlight of the one-week course, which was dedicated to encouraging critical thinking and constructive debate between different points of views, was picking the winners of the Cyber Security Challenge.

The challenge involved project assignments with each group assigned a different task. The "Dark Web" team received the "Best Team Effort" award and two students received the nod for Best Individual Effort.

By Livia Jusztin-Majercsik, Chief Strategy Office.

Student Testimony - Michael Reiner

I was extremely impressed by the programme's diversity. This unique partnership, infused by collaboration with other international organisations bridged the natural divide between military, law enforcement, industry, academia, researchers, and policy makers.

With 61 students of 24 nationalities – ranging from students to young professionals with technical, policy, and legal backgrounds – the diversity of the ICSSS was palpable every step of the way!

We were immediately put to the test when the course started: we were divided into groups, presented with a cyber security game, and asked to collaborate to achieve common goals.

Throughout the week, we broadened our understanding of innumerable cyber topics through presentations and practical demos from experts. We were assigned to different teams with dedicated instructors from the NCI Agency, Europol, and NATO Cooperative Cyber Defence Centre of Excellence. The workshops covered IPv6 security, cryptocurrencies, dark web, web security essentials, and hacking with software-defined radio. At the end of the week, we presented our findings and lessons learned before the whole class;

Awards were bestowed upon the best team and best individuals. But the learning experience was not limited to the classroom environment. After class, we regularly had planned activities, we networked with former ICSSS alumni and with current students of the National Cyber Security Summer School. We spent the few remaining hours of our evenings together, heading to the beach and nearby establishments; we probably only slept five hours per night.

The atmosphere of the course was not overly formal, which greatly contributed to forging lasting relations with students and instructors alike.

Overall, the ICSSS experience was extremely gratifying – both personally and professionally. On the last day, it was difficult to say goodbye to those we shared this wonderful experience with – some of us could not hold back the tears but we return to our countries with a greater network of trusted peers which I look forward to meeting in future cyber security endeavours!

ALL HANDS ON DECK:

Supporting NATO and national operations in the Aegean Sea

NCI Agency CIS Support Element (CSE) Athens has been tasked with a pleasant assignment - establishing itself as an attractive service provider in Greece.

Located in the birthplace of democracy, CSE Athens was established in 2014 with the mission of installing, operating, maintaining and supporting the full range of Communications and Information Systems (CIS) capabilities in its allocated Area of Responsibility.

The CSE's core tasks are mostly defined by its parent sector, the Agency's CIS Support Unit (CSU) Naples in Italy.

The existence of a NATO Communications Unit, in the current location of CSE Athens, dates back to 1982 when it was first established as the Local Control Organization (LCO) Athens. It then operated as the Allied Signals Group Athens from 1999 and the Athens Communications Squadron from 2004.

It became the NATO CIS Support Element in February 2014.

After its activation ceremony, which took place on 26 May 2014, CSE Athens started anew under the leadership of the Agency.

Over the last two years, the CSE has had to build relationships with the Nations from scratch and provide NATO CIS services to local customers.

It has had to fulfil these ambitious tasks while the Service Level Agreement was still under negotiation. And at the same time, the CSE has had to cover services previously provided by the NATO Communication and Information Systems Services Agency Detachment Larissa after its closure in September 2013.

Despite these challenges, the first Commander of CSE Athens, Lieutenant Commander Fotios Katsantas, faced the new state of affairs with undivided attention and optimism.

Indeed, he piloted the ship through uncharted waters with confidence despite the length of the journey, like Ulysses who endured 10 years of strife before reaching his safe harbour in Ithaca: his family.

The Commander's approach to success also involved a family of sorts – a team of experts based in Athens.

His goal was to develop and maintain team spirit, as well as interpersonal relationships among staff. This was successfully accomplished as the CSE Athens established itself as the Agency's focal point in Greece.

Since then, the CSE has continued to provide CIS and 24/7 Control Centre and Helpdesk services to numerous local customers such as the NATO Rapid Deployable Corps – Greece, and the Greek Ministry of Defence, and all Greek Ships participating in NATO and multinational exercises and operations in the Eastern Mediterranean and in The Persian Gulf.

In the last couple of years, the team has faced several challenges of varied difficulty. As a new Agency CSE, Athens had to create a proper working environment for its personnel. This meant working in buildings under construction while maintaining the provision of high quality services.

Although CIS services are technical by nature, they heavily rely on proper communication and collaboration among teams and stakeholders. This is a challenge each CSU has had to overcome in order to succeed.

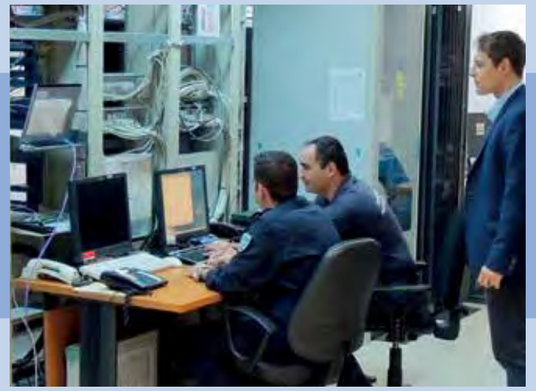
A happy occasion for CSE Athens was successfully hosting the NCI Agency Commanders Conference in November 2015.

Looking to the future, CSE Athens would like to establish and expand its presence in its Area of Responsibility, by gradually improving the services it provides. Although it is a small team, CSE Athens plays a pivotal role with its thorough knowledge of the region's CIS terrain.

It acts as the single point of contact for local customers, resolving underlining problems as they arise.

This communication role is of vital importance. Since relationships affect actions, and actions affect relationships in all business areas, a single customer interface can solve a lot of underlining problems.

By Fotios Goulousis, CSE Athens.



ACCS

PROTECTING NATO'S AIRSPACE

This year, the Combined Air Operations Centre for Northern Europe in Uedem, Germany (CAOC Uedem) became the second site across the Alliance to start using the Air Command and Control System (ACCS) for its operations.

ACCS is NATO's most valuable programme to date, and will cover 10 million square kilometres of airspace when fully deployed.

This advanced system, supported and maintained by the NCI Agency, integrates such functions as aircraft control, air traffic control, command and control and airspace surveillance among others.

It will eventually replace national and NATO systems, interconnecting more than 20 military aircraft control centres in Europe.

"The most important thing is that we provide [with ACCS] a picture to link between the tactical and the operational level," said MGEN Dré Kraak, Commander of Deployable Air Command and Control Centre in a newly-released NCI Agency mini-documentary which can be found on our YouTube channel.

"So what we do here, the picture that we provide with ACCS can be linked directly to the higher headquarters so they know what's going on and they can take their decisions based on what ACCS and our system is providing."

By Creative Media Centre.

Subscribe to the NCI Agency channel on YouTube

NITEC:17

NCI Agency's 2017 Annual Conference to Focus on Innovation

'Innovation' has become the watchword for many defence organizations as they confront fast-evolving security challenges and rapid technology design in the private sector, where more commercial technologies than ever before have military applications.

For the NCI Agency, these new realities have raised the bar on what it takes to maintain the resilience of our communications and information systems, resulting in a continuous need for innovation.
Harnessing the innovative capacity of Alliance Industry to help make NATO networks more resilient will be the focus of NCI Agency's annual flagship conference, NITEC17, with the theme of "Sharpening NATO's Technological Edge: Adaptive Partnerships and the Innovative Power of Alliance Industry."

The annual three-day event, which is organized jointly with AFCEA Europe (the Association for Communications, Electronics, Intelligence and Information Systems Professionals) and in collaboration with Host Nation Canada, will take place on 24-26 April 2017, in Ottawa.

The conference comes as Alliance Heads of State and Government reinforced the imperative of supporting innovation through greater collaboration with Industry during the 2016 Warsaw Summit.

NITEC17 will offer a unique opportunity to act on NATO's innovation agenda through strategic dialogue with Industry partners about the applicability of advanced and emerging technologies in the military domain and new thinking about how to implement them.

"Over the past year, we have heard repeated calls—including at NITEC16 in Estonia—for a shift from government-issued requirements to team-built capabilities, where government and Industry teams work together at earlier stages to solve problems and deliver solutions," NCI Agency General Manager Major General (ret) Koen Gijsbers said.

"NITEC17 will be an ideal platform to continue moving forward with this new approach."

Bringing together more than 500 high-level defence experts from across NATO, the Allied militaries, Industry and academia, NITEC17 will build upon the success of NITEC16.

While NITEC16 established a clear consensus about the need for partnership and innovation, NITEC17 will focus on converting that consensus into action. This will require focusing on innovative processes in addition to technologies—a key message of NCI Agency Director of Acquisition Peter Scaruppe during remarks at an innovation forum in Canada which took place in November 2016.

"The cutting-edge technology we need to stay ahead of our adversaries is out there," Mr Scaruppe said, adding that the Agency needs to apply innovative approaches to tap into the innovation that companies across the Alliance are doing every day.

The Agency's robust innovation agenda is aimed at accessing more innovation from more sources more rapidly, with several new initiatives piloted this year.

These include a cyber acquisition reform study that will produce recommendations for improving NATO's cyber procurement processes and a mentoring program for small and medium enterprises to receive advice from larger companies on partnering with NATO and other topics.

A Defence Innovation Challenge aimed at tapping the technology solutions of SMEs and academia across the Alliance was also introduced in 2016.

Meanwhile, the NCI Agency held four Threat Vector Analysis workshops with Industry partners this year through the NATO Industry Cyber Partnership (NICP).

It has completed the pilot phase of the NICP Malware Information Sharing Platform, and doubled the number of bilateral Industry Partnership Agreements on cyber information sharing, bringing the total to eight. At NITEC17, the Agency will launch a Next Generation Innovators Programme aimed at preparing the next generation of information security experts.

Business opportunities

On Day One of the conference, senior decision-makers will discuss key trends in the innovation landscape, how they are re-shaping traditional government-Industry collaboration, and the implications for NATO.

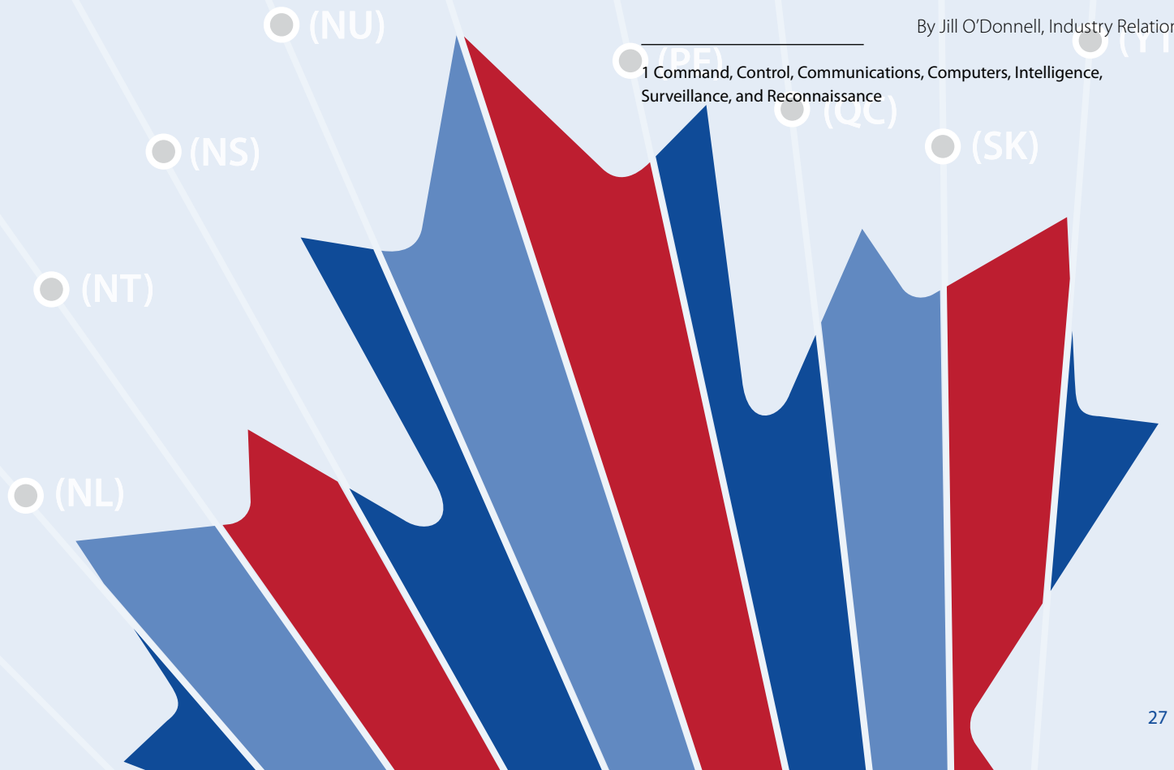
Days Two and Three will offer a forum to discuss with Industry the NCI Agency's 3 billion EUR worth of business opportunities planned between now and 2019 in cyber, air and missile defence as well as advanced software. This includes a 70 million EUR investment in cyber technology focused on secure mobility, multi-level authentication, and secure use of public clouds.

In order to stimulate actionable priorities, simultaneous break-out sessions of smaller groups will consider focused questions—including those that arise from Day One sessions—on the challenges and opportunities of re-fashioning NATO-Industry collaboration to speed innovative solutions.

In addition to the AFCEA Technet International exhibition, B2B meetings and networking opportunities, the NCI Agency will continue two well-received initiatives that were launched at NITEC16, the Defence Innovation Challenge and SME Mentoring Programme. Both programmes are aimed at accelerating transformational, state-of-the-art technology solutions from small business and academia in support of NATO C4ISR[1] and cyber capabilities.

By Jill O'Donnell, Industry Relation

1 Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance



The MESSENGER of the Sea

Named after the messenger god of the sea, NATO's project Triton aims to provide one single platform for maritime missions.

One single messenger

NATO Maritime Command and Control (C2) Information Services currently consist of a number of operational systems, which are used by different Nations and Commands on various platforms. The lack of a consolidated system has prevented maritime operations communications from being as seamless as they could be. Project Triton, which is being acquired by the NCI Agency as Host Nation, aims to remedy this situation.

This NATO common-funded project is within the Bi-Strategic Command Automated Information System architecture, and aims to replace the current aging systems. Triton covers all procurement and implementation activities in support of Maritime C2.

Full mission spectrum

Triton services will provide the tools for NATO operational users to plan and execute the full spectrum of maritime missions in a joint environment. They will enable the operators to share a common view of the battle space, improving their situational awareness and decision-making processes.

Once the project is procured through International Competitive Bidding, the road for future growth will become wide open. Triton's first Increment will aim to collect maritime track information from NATO sources and Nations to build a Recognized Maritime Picture depicting all military maritime activity, and to collect data from commercial sources to build up a White (Shipping) Picture, to map the traffic of merchant vessels.

Among further improvements, Triton's second Increment will focus on Maritime Operational Planning and Execution, and the complete implementation of Naval Mine Warfare Planning, Execution and Evaluation.

Accessible beyond borders

Triton will be a centralized, web-based application allowing operational users from the NATO Command Structure and National Headquarters to access its functions from any location.

It will first be tested and evaluated during ongoing operations and exercises by Maritime Command (MARCOM) in Northwood, UK.

The tool providing imagery for Triton will be delivered as a re-usable software component, so that it may be used for mapping and user interface in other C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) systems as well.

Testing the messenger in collaboration

The NATO Centre of Maritime Research and Experimentation (CMRE) in La Spezia, Italy, will provide basic research and prototype development support which will then be formally applied during the implementation of the project.

Meanwhile, NCI Agency, SHAPE, ACT and MARCOM users are participating in conferences, workshops and working groups to adjust the system's specification and implementation process during its test phase.

Once live, the Agency will be responsible for providing lifecycle support, with the CIS Support Unit Northwood taking on the critical role of providing primary support to the Maritime Community.

Stronger together

Once Triton is tested and fully procured, it will be a common platform for monitoring military maritime activities throughout the entire Alliance. Nations and Commands will be able to share their maritime operations and exercises information live, in a consolidated system, so that Triton can live up to its name and become a true Messenger of the Sea for NATO and its Partners

By Erhan Saridogan, Command and Control Services.

WHAT MAKES A GREAT (CYBER) LEADER?

Winner of SC Magazine's 2016 CSO/CISO of the Year, NCI Agency Chief of Cyber Security Ian West told the Communicator what makes a great cyber leader.

Both you and your team were nominated for the prestigious SC Awards 2016 Europe. It is quite a compliment, were you surprised?

SC Magazine is probably the leading cyber security publication in the world, it represents all aspects of the cyber security spectrum and is relevant to all organizations, from Industry to governments and academia.

So to find out first of all that I'd been nominated for this [Chief Security/Information Security Officer] award was quite a shock, and a very pleasant shock.

It's quite an accolade, and clearly not just for myself but it is also a validation that what we do in NATO is being recognized and is seen as being successful, and it is clearly important.

Then we were told a little bit later that the cyber security team had been nominated for an award as well, that was more important to me, because there are 200 people who are doing a great job – and it's not just the people in the cyber security service line, we are supported by a whole range of folks from other parts of the Agency.

So winning these awards was incredibly important not just for those of us involved but to NATO as a whole. It really is that significant because when I talk about the team, everything that we do is guided by the [NATO Member] Nations. And the Nations over the years have shown supreme commitment to cyber defence with lots of initiatives at every Summit. It is a very big NATO team.

The recognition is made all the more special because the Awards were judged not just by SC Magazine, there was a panel with 25 experts from academia, Industry and government organizations so it's a huge honour and a great privilege to be a part of it.

What does it take to be a great cyber leader?

There is a phrase: 'From server room to boardroom." And basically what this means is that you can be the best technician anywhere, but if you cannot explain to the boardroom why they need cyber security, then you are probably not going to be successful.

So the really important thing is engagement with and communication across the whole organization, all the way up to our boardroom. It is really important to facilitate this interaction.

The other thing that we've learned is that nobody has the entire solution for cyber security, everybody has a piece of the jigsaw.

Of course, NATO has recognized this, you've got to work together, it's got to be a collective effort. That's why we work very closely with our Allies, our Partners, Industry and Academia, as well as the EU. Working together really does enhance our collective cyber defence.

By the way, in February 2016, we signed the first formal agreement between NATO and the EU in years. It was signed between the NATO Computer Incident Response Capability, (NCIRC) which of course is part of the Agency, and the Computer Emergency Response Team – European Union (CERT-EU). There is a lot of commonality between the EU and NATO, particularly as we use similar technology and face the same cyber threats, so working together for the common goal is a win-win situation for us.

A cyber security leader must understand not just the importance of cyber security itself but how it should work within an organization and even globally.

Should every organization and company have a cyber security team then?

The worst thing you can do is just implement very expensive technology, and get very scarce and expensive skills without knowing why you are doing it and what you are trying to protect.

You've got to identify what is critical – the critical components of a company's network or an organization's computer systems, communications systems – and then place the most security on the most important parts of those.

Now every organization – whether it's governmental, commercial, academic – that depends upon its computer network must have some form of cyber protection. And clearly if it's a smaller company or if the dependency is say less than that of a bank, then they'd need less of a solution but focused on their 'crown jewels'.

But everybody, every organization that depends on its networks has to have cyber security embedded into it.

What advice would you give to young new leaders who may work in other areas than cyber security?

There is a simple leadership principle that I was taught when I was in the UK Royal Air Force and it's that true leadership is about finding the optimum between three components: the mission – 'getting the job done' - looking after the team, and looking after the individual.

If you imagine three overlapping circles, if you concentrate too much on the mission without looking after your people or creating a team, then they are probably not going to be able to complete that mission.

You've got to find the middle of these three overlapping circles and look after the team and the individuals to make sure that the mission gets done.

I am very lucky that I work with very special, skilled and dedicated team-mates. We went from having a team of about 80 people to having a team of 200 people and I just about know everybody's name now. But it's not only about understanding what they do and knowing what their names are. You've got to know the people, you've got to know their capabilities, their shortfalls, their ambitions, their circumstances.

Now, obviously I work with some other great managers and it's just impossible for me to do all of that for 200 people. But it's an ethos of mine that we do look after our people. They are part of that triad if you like. I am also lucky that our cyber security team is incredibly dedicated to the mission. Perhaps it is because it is very real. Every day, they are defending against real threats. They know that if they miss one attack, the effects to the Alliance's operations and business.

Interview by
Lucie Cimoradska, Chief Strategy Office
and Adelina Campos de Carvalho, Creative Media Centre.

A CHANGED MAP…

reinforces old truths

In July 2016, 28 Presidents and Prime Ministers (and lots of staff and journalists) took over Poland's national football stadium.

NATO's Warsaw Summit changed the Alliance's map in unprecedented ways. And yet, after the Summit, the core challenges faced by the Agency, NATO's advanced technology provider, are oddly familiar.

Land, sea, air…

…And cyber. The first map that changed following Warsaw was that of the Alliance's operations which gained a new dimension – cyberspace. Our Heads of State and Government recognized cyberspace as a new operational domain for the Alliance.

The Warsaw Summit also changed the Alliance's capability map. NATO's ballistic missile defence reached Initial Operational Capability, which was a major milestone and success for contributing Nations, international staff, Commands, as well as the Agency and Industry Partners.

The cooperation map shifted too. The Secretary General signed a Joint Declaration with the Presidents of the European Council and the European Commission, taking partnership between NATO and the European Union to a new level. The Alliance agreed to significantly step up the support it provides to our Partners in North Africa and the Gulf, helping them better defend themselves and fight terrorism and extremism in their region - for instance through capacity building of the Iraqi armed forces.

From immediate response to long-term adaptation

Perhaps the most visible aspect of this new map has been NATO's defence and deterrence posture. The 2012 Wales Summit was about an immediate response to the rise of the so-called Islamic State of Iraq and the Levant (ISIL)/Da'esh and Russia's illegal annexation of Crimea. In contrast, the 2016 Warsaw Summit was about ensuring a long-term strategy, a two-track approach, one that combines strength with dialogue.

This year, Allied Heads of State and Government agreed to enhance NATO's forward presence in Estonia, Latvia, Lithuania and Poland and to develop a tailored forward presence in the Black Sea region. To the south, in addition to capacity-building measures already mentioned, NATO launched a new maritime operation, Sea Guardian, and deployed AWACS aircraft to support the counter-ISIL coalition.

Just the beginning?

Speaking recently, former Deputy Secretary General, Ambassador Alexander Vershbow, gave examples of further *"homework"* for NATO post-Warsaw. For instance, he mentioned a *"functional assessment"* of the command structure; the establishment of a full-time Assistant Secretary General for Intelligence and Security at NATO HQ as a means of upgrading the role of intelligence in our decision-making and our military planning.

He also suggested homework for the NATO countries themselves: *"At home, Allies also need to work on their resilience".*

"They need to ensure they can withstand hybrid attacks and be able to continue to function in a crisis situation. This requires a 'whole of government' approach as it touches on infrastructure, continuity of government, defence against cyber-attacks, the ability to deal with mass civilian casualties, the ability of NATO forces to cross and operate on the territory of Allies," Ambassador Vershbow stressed.

So what?

More work. Since Warsaw, the Agency has already had to increase its output to support NATO's new commitments: for example technology support to the AWACS' anti-ISIL mission, supporting NATO's maritime command with its new commitments, or rapidly delivering connectivity for the Enhanced Forward Presence in the East. It's not just more work, the nature of the work is changing as well.

First, there is a greater focus on multinationality and interoperability at a lower, even tactical level. As the Secretary General stressed: *"Our forces will be truly multinational. Sending an unmistakable message: NATO stands as one. An attack on any Ally will be considered an attack on us all."*

Second, resilience. Ballistic Missile Defence on NATO's networks to link national sensors and interceptors. These networks cannot fail.

Cost pressure

Our customers therefore face a twin challenge – the increasing role of IT (and therefore more demand for IT) while facing significant budget constraints.

So an old challenge will return in this totally new map: the drive for efficiency, working in partnership with Industry to deliver, where possible, at a reduced cost. Although 2016 saw the first ever increase of European defence budgets, the mismatch between ambition and funding is likely to remain, and with it, pressure on the Agency.

Implementing innovation… rapidly

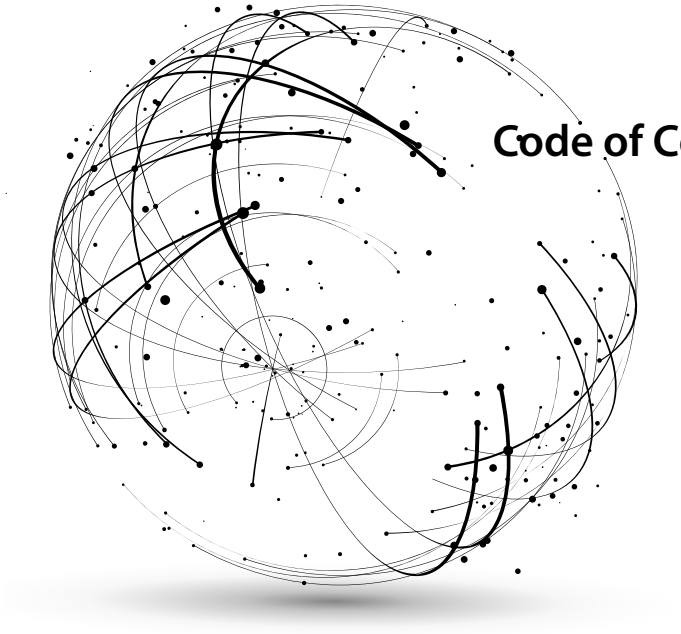
The world will not stand still (see the Technology Watch article). The challenge is two-fold, not only must we innovate as fast as (if not faster than) our adversaries, but we must also reexamine the way we innovate.

We should end on a note of caution. Staffs at NATO's political and military headquarters and in capitals are still working on all the taskings from the Summit.

Nonetheless, it appears to be a safe wager that on this new, post-Warsaw map we will encounter two well-known friends: the need to innovate more rapidly than before and the financial pressure to deliver more while reducing costs and significantly increasing efficiency.

Daunting? Perhaps. Impossible? No - the key ingredients are already well present in the Agency: brilliant people, strong partnership with Industry and the mindset and courage to do what has not been done before.

By Michal Olejarnik, Chief Strategy Office.



Code of Conduct for NATO CIS privileged users

A new Agency Directive has been drafted to ensure that sensitive data is protected from cyber threats.

Classified

Directive

Route

This Directive applies to privileged NATO network users who, by virtue of their function, have access to information other than their own. This Directive generally applies to staff tasked with securing, handling and monitoring the NATO CIS networks, such as a local System Administrator, a Data Analyst or any other user holding privileges, rights or permissions on NATO CIS.

Privileged users have access and means on the NATO CIS that go beyond those of a normal user. For this reason, and in view of their function, these users have greater responsibilities than that of a normal NATO CIS user.

Therefore, an Agency Directive has been drafted to provide these privileged users with guidelines, ensuring that the privileges granted to them are used in an appropriate manner.

Data

privilege

The Agency Directive aims at setting up minimum requirements for privileged users. It does not waive or undermine stricter requirements such as those found in any Security Operating Procedure or similar documents, or any requirement for appropriate security clearances. The Directive will apply to personnel, including those of other NATO entities, commercial contractors or any other personnel who require such privileges to perform their duties.
In their duties, privileged users have for example the ability to access information at the highest level of classification within the specific CIS, as well as access any other type of information not usually available to users. It is therefore important to have a system of checks and balances in place in order to ensure that no abuse will occur, or no undue benefit can be drawn from their position.

User

As an example, a guideline has been set up to make sure that certain critical actions on NATO CIS require the agreement of two privileged users (two men rule), thus providing an extra check. Another example of a guideline which can be found in this Directive is that a privileged user shall always prefer the least intrusive method to carry out his/her function. If the same result can be achieved by intrusive or non-intrusive means, the latter will be preferred. Moreover, privileged users are always required to take actions only in line with their assigned tasks; any activity undertaken by them may be monitored and logged for audit or investigative procedures. This means that, although it should not occur frequently, one can be held accountable in case of abuse of privileges or through the gain of undue benefits.
The directive will be implemented under the auspices of the Agency Security Manager.

Monitored~..

By Office of the Legal Advisor.

NIAS CSS'17

CYBER SECURITY SYMPOSIUM

Save the Date

17 - 19 October 2017

Mons, Belgium

NATO Communications and Information Agency
Agence OTAN d'information et de communication

Bâtiment Z
Avenue du Bourget 140
1110 Brussels
Belgium
www.ncia.nato.int