C COMMUNICATOR

Issue 2 | 2017

A HISTORY

of NATO support

MEET KEVIN SCHEID

NCI Agency's new General Manager

NATO
OTAN

NCI
AGENCY

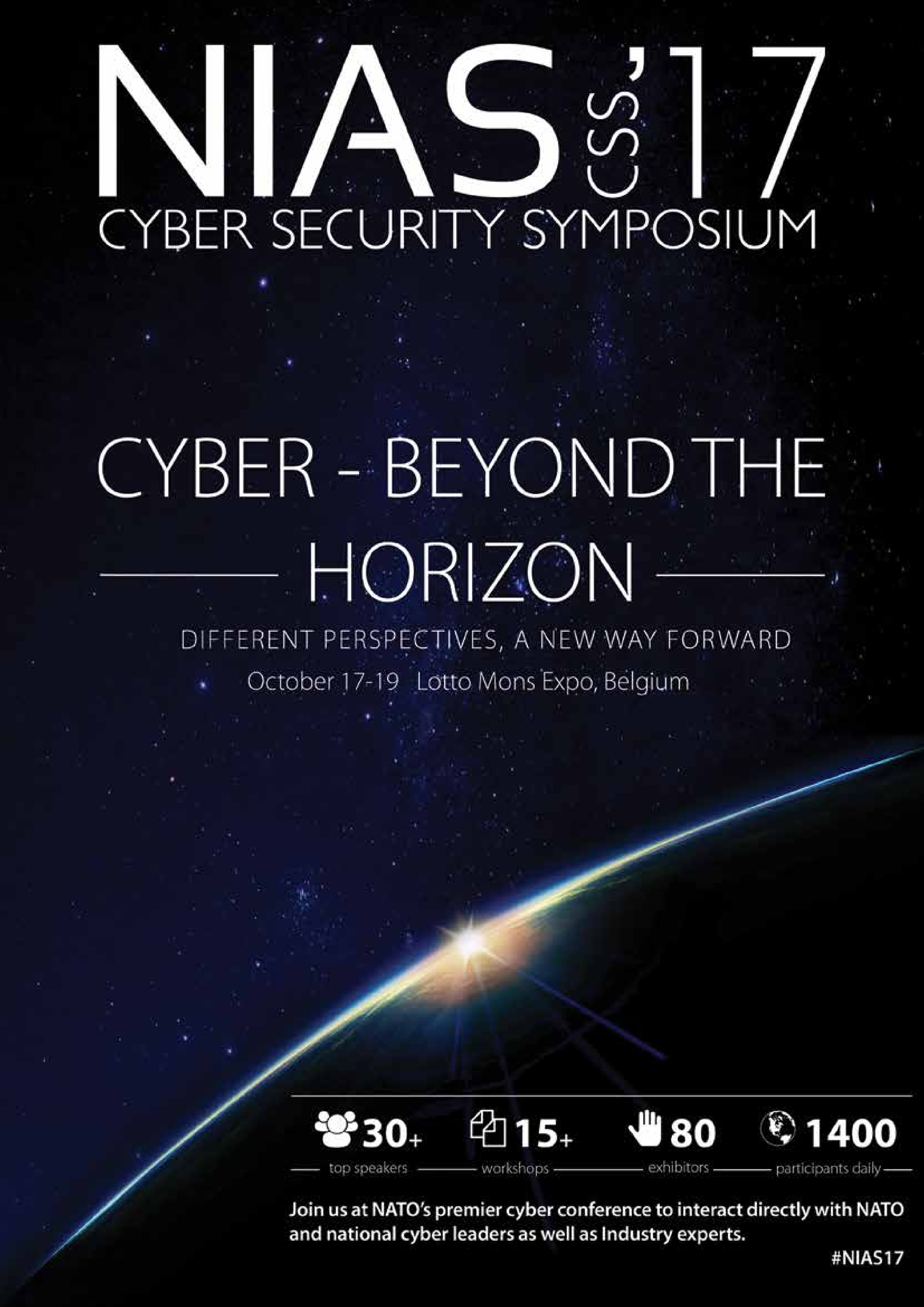


Table of contents

4 Foreword by Koen Gijsbers: Stronger together

6 Dobrodošao Montenegro

8 Technology Watch: Quantum Leap

11 A history of NATO support

18 The Agency in Norfolk: Connected today for the partnership of tomorrow

20 Strength in numbers: Supporting the Afghan mission

22 Conversation with Kevin Scheid, the NCI Agency’s new General Manager

28 BALTOPS, a NATO maritime exercise with 46 years of history

30 Defence Innovation Challenge winners

33 NATO breaks ground on C4ISR and cyber Academy

34 Defending a smart city: Federating civil, military things and data

36 Laying down the (cyber) law

Chief editor
Michal Olejarnik

Deputy editors
Adelina Campos de Carvalho
Lucie Cimoradska

Layout, Design & Print
NCI Agency - Creative Media Centre

Contributors
Please see articles

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

Stronger together

Koen Gijsbers' parting thoughts as he hands over the baton to Kevin J Scheid.

I am frequently asked: "How did your 4 x 400 meters record last so long?" One answer is, it took four strong runners, not just one.

The current holders of the world record, the US team, has since bested our time from the Mexico 1979 World Championships by 8 seconds, but we held the Netherlands' 4x 400 m record for 38 years – until this year.

My point is that good teams have more value than the simple sum of their parts. Take the NATO Alliance. You can break one Nation. It is much more difficult to break 29.

It begins in the mind

When you are at the Olympics, there is little that separates you from the other athletes physically. It is your mindset that determines whether you win or lose.

Building teams is not dissimilar. You begin the journey by accepting that you can learn from others, listening as much as passing on information. Easier said than done. But over the last five years – since the birth of the NCI Agency in Afghanistan on 1 July 2012 – I have seen our team grow together and make NATO stronger.

Take the worldwide WannaCry ransomware attack, the NCI Agency's cyber experts could immediately task our local teams in over 30 locations to apply critical patches, because they all belong to one organization. No time was lost in discussion or coordination. Factories were shut down during the cyber-attack, caesarian births and operations had to be postponed, but NATO, this time, was unaffected.

A wider roster

There are other examples. Since 2012, we bring under one roof the teams that develop NATO software, those that operate the infrastructure on which that software resides, as well as those that write our contracts with Industry. This allows for synergies.

Why does this matter to NATO? Because these synergies allowed us to connect the anti-missile defences deployed to Turkey in two weeks, or NATO's eight new headquarters in Central and Eastern Europe in record time. Clever thinking by our engineers gave NATO speed. A stronger Agency makes a stronger NATO.

For me, the single most important achievement of the last five years is getting what were previously five different organizations to see that they can deliver better services to the Alliance as one team, getting them to appreciate the value in one another's contributions.

Diversity is gold

A common culture does not need to mean a fully homogeneous culture. Tension is good. The qualities that make one person an ace fighter pilot will not necessarily make someone else a good air defence planner.

Today, most corporations consciously seek to build diverse workforces with some underlying tensions bound by a common purpose. We should argue, we should have differences of opinion. But when we run, we run together, as one.

Shaving seconds

For we are not the only ones in the race. Our adversaries are trying to beat us to the finish line. The world around us does not stand still. Even the track changes.

When you begin training for any sport, the initial gains in performance are relatively easy to achieve. You replace three General Managers with one, you get savings, and you start bringing teams together.

But as you begin to push up against your limits, those gains become increasingly hard to make. Shaving seconds off your time is much more difficult than losing the first few minutes.

The Alliance depends on IT now more than ever before. As I pass the baton, I will be cheering loudly from the stands. This wonderful team has, for the good of NATO, a very important race to run.

It has been an honor to run with you for the first five years.

Koen Gijsbers, General Manager (2012 - 2017)

Dobrodošao Montenegro

Connecting NATO’s newest Ally

As Montenegro became NATO’s newest Member Country this June, the NCI Agency connected the Balkan Nation to the rest of the Alliance. It was the Agency’s responsibility to ensure that Montenegro’s capital Podgorica would have a direct link to NATO’s political and operational hubs, the NATO Headquarters in Brussels, and Supreme Headquarters Allied Powers Europe (SHAPE) in Mons, Belgium.

Jonathan Copner, who managed the ‘CIS for Montenegro Accession’ project, explained that every new Ally is offered a ‘Welcome Package’ when they gain membership. This includes basic CIS capabilities that are required to participate in NATO consultations.

However, Montenegro was a special case. *“Most of the Nations that have joined so far have had their own national capabilities, and all we have done is establish a gateway to allow their secret networks to interconnect with NATO, and then they handled the rest of it. Montenegro is slightly different. Being a small Nation, it doesn’t currently have its own secret network capabilities. So we proposed a multiple phase approach.”*

Sharing NATO expertise

The Agency provided a basic secret Communications and Information System (CIS) to Montenegro, as well as two Air Command and Control capabilities integrating NATO’s new member in the Allied air picture.

“The first phase was to simply extend NATO services, to provide them with a basic capability. So, we didn’t interconnect their own networks, what we did was extend NATO’s secret network to a limited number of positions in Montenegro within the Ministry of Defence, the Ministry of Foreign Affairs, and their Air Operations Centre.”

It only took several weeks for the 29th Ally to be ready to participate in NATO consultations, but the Agency’s support didn’t end there. NATO’s newest member is already preparing a request to extend this initial setup with further work stations and sites.

“The Welcome Package was funded by NATO, while Montenegro is responsible for paying the Agency’s ongoing support costs. So, NATO paid for the entry points, but all further capability development will be funded by the Nation itself. When conditions are right, and when Montenegro is ready to build its own national secret network, the Agency will deliver the second phase of the project.

This will allow Montenegro to transition to the model used by other NATO Nations where all we do is maintain the gateways. For now, we have no anticipated date for the second phase, we will take our cue from the Nation,” Mr Copner added.

The project team has been working with Montenegro since last year to ensure a smooth transition from Partner to Member Country.

Continuous support

“My first involvement with Montenegro was in September 2016, with initial site surveys and participation in an ongoing Accession and Integration Working Group. The Working Group meetings have been taking place throughout the last two years, and will continue, because it is not only about establishing Montenegro within NATO, but also looking at developing their capabilities, and integrating them as they move forward. Accession is only the first step of that,” Mr Copner added.

“We received the project authorization in November 2016, and delivered the CIS required for accession ahead of the formal ceremony. The project was delivered on time and within budget. “

Montenegro became a full NATO Member in June 2017, but the journey of defence capability development is just beginning.

“It became clear that we needed to share with Montenegro our experience and NATO’s best practices for protecting CIS, in terms of understanding the NATO policies and procedures of secure networks. We have spent a lot of time working together on the procedural level. A representative of Allied Command Operations and myself headed back to Montenegro during the week of their accession to ensure that all went smoothly, and to be certain that, before the secure networks went live, all of NATO’s various security requirements were met.”

By Livia Majercsik, Chief Strategy Office

Quantum Leap

Welcome to the third instalment of Technology Watch where each issue, we take a look at an emerging technology that we believe will have a significant impact on Allied capabilities in the coming three to five years. In this issue, we look at quantum technologies.

What are quantum technologies? The name comes from breaking down anything - light, matter and energy – into its smallest possible unit, a unit called a "quantum" (plural, quanta). At this scale, all objects stop behaving in the ways we're used to, the ways classical physics describes them. Instead, quanta behave in ways that are difficult to comprehend. They often behave as if they're two things at once, for example, a photon (a quantum of light) behaves as if it is both a particle and a wave.

This results in quanta having two properties which have huge potential to transform technology. The first is that, at this scale, objects can be in two states or places at the same time (known as superposition); the second is that two quanta can affect each other even though they are far apart (known as entanglement).

Both superposition and entanglement have the potential of transforming many aspects of our business in the future.

Quantum computing and decrypting data

Superposition and entanglement offer tremendous possibilities for computing. Whereas classical computing uses units – 'bits' – which are either a "0" or a "1", in a quantum computer, the quantum bits – 'qubits' - can be both 0 and 1 at once. This phenomenon, coupled with algorithms for quantum computing allows certain problems to be calculated with a much lower level of computational effort.

Communications systems remain secure by making it prohibitively difficult to decrypt the transmitted information without access to the key.

Variants of public key encryption (where everyone can see the public key which is used to encrypt the data, but only the recipient has access to the private key which is needed to decrypt it) rely on it being too difficult to calculate the private key to decrypt data, even when someone has the public key. As the key gets longer, it becomes exponentially more difficult to attack.

Attacking public key encryption involves a lot of computationally-intensive searching and factoring of large numbers. With traditional computers, these functions are very time-consuming, even for modern processors. So the security of public key encryption relies on searching and factoring numbers being very complex. However, algorithms for quantum computing that exploit the superposition property of quantum computers have dramatically changed this.

A quantum computer can attack public key encryption much more effectively, drastically reducing the security of communications systems.

For example Shor's algorithm can quickly factor numbers, while Grover's algorithm speeds up searches.

As factoring and searching are exactly the functions which make public key encryption so secure, advances in quantum computation, such as these algorithms, cryptographic problems which were difficult and not solvable in reasonable timeframes using conventional computing, have become fairly trivial problems for a quantum computer. Across the defence industry, it is evident that quantum computing poses a credible threat to some security mechanisms currently in use. In fact, it makes some of our current generation encryption technologies obsolete. In some cases, quantum computing effectively halves the length of the key.

As quantum processing power increases and programming techniques advance, the threat to eavesdrop on traffic, or to decrypt historic data grows significantly as well.

Quantum safe cryptography

Does quantum computing mean all encryption is compromised? Not completely. There are challenges to manufacture quantum processors which are effective against current algorithms. But state-of-the-art technology is advancing rapidly and the true capabilities available in most research labs remains secret (especially in some government research facilities).

To counter the threat posed by quantum computing, the concept of 'quantum-safe cryptography' has developed in recent years. This uses encryption algorithms in conjunction with other mathematical functions to encrypt data in ways which are difficult for quantum computing to analyze. Quantum-safe algorithms have been developed, and equipment using these algorithms is beginning to become available commercially.

In 2015, a small company specializing in quantum-safe cryptography participated in the NCI Agency's cyber security technology incubator, as part of the Agency's Innovation Programme. PostQuantum Ltd produced a messaging App which protects data with a quantum-safe algorithm and additional security features. PostQuantum Ltd is now delivering quantum safe cryptographic products to commercial telecom operators, IT providers and the finance industry.

Quantum communication

While quantum technologies pose a threat to encryption, they offer a solution to another communications challenge – detecting whether your communications have been compromised. Whenever an unknown quantum state is measured, the state changes in some way. This provides a very useful property to identify if communications have been intercepted and it is exploited in Quantum Key Distribution (QKD).

QKD is the first quantum technology to emerge in commercial use. Civilian standards for QKD are already being developed by the European Telecommunications Standards Institute (ETSI) and others, while companies such as IDquantique offer commercial services.

QKD exploits the entanglement property of quantum mechanics to securely distribute keys for conventional communication - the most sensitive element of the communication process. Conventional security mechanisms (often employing quantum-safe cryptography) are then used to protect traffic transmitted conventionally.

The same quantum principles of QKD can be applied to the entire communication network. A 2000km quantum communication link now operates between Beijing and Shanghai demonstrating the concept is viable for long distances. In August 2016, China also launched a satellite purported to be able to generate and distribute quantum encryption keys from space.

Most current technology addresses point-to-point communications, as using this technology for many-to-many network connections is complex. However, there is significant research activity in this area from both the government and commercial sectors, so rapid advances will happen.

And as the use of QKD becomes more widespread, this tool, while useful for national and international defence, could also pose a threat to our societies as it offers our adversaries coding techniques that are guaranteed to be unbreakable.

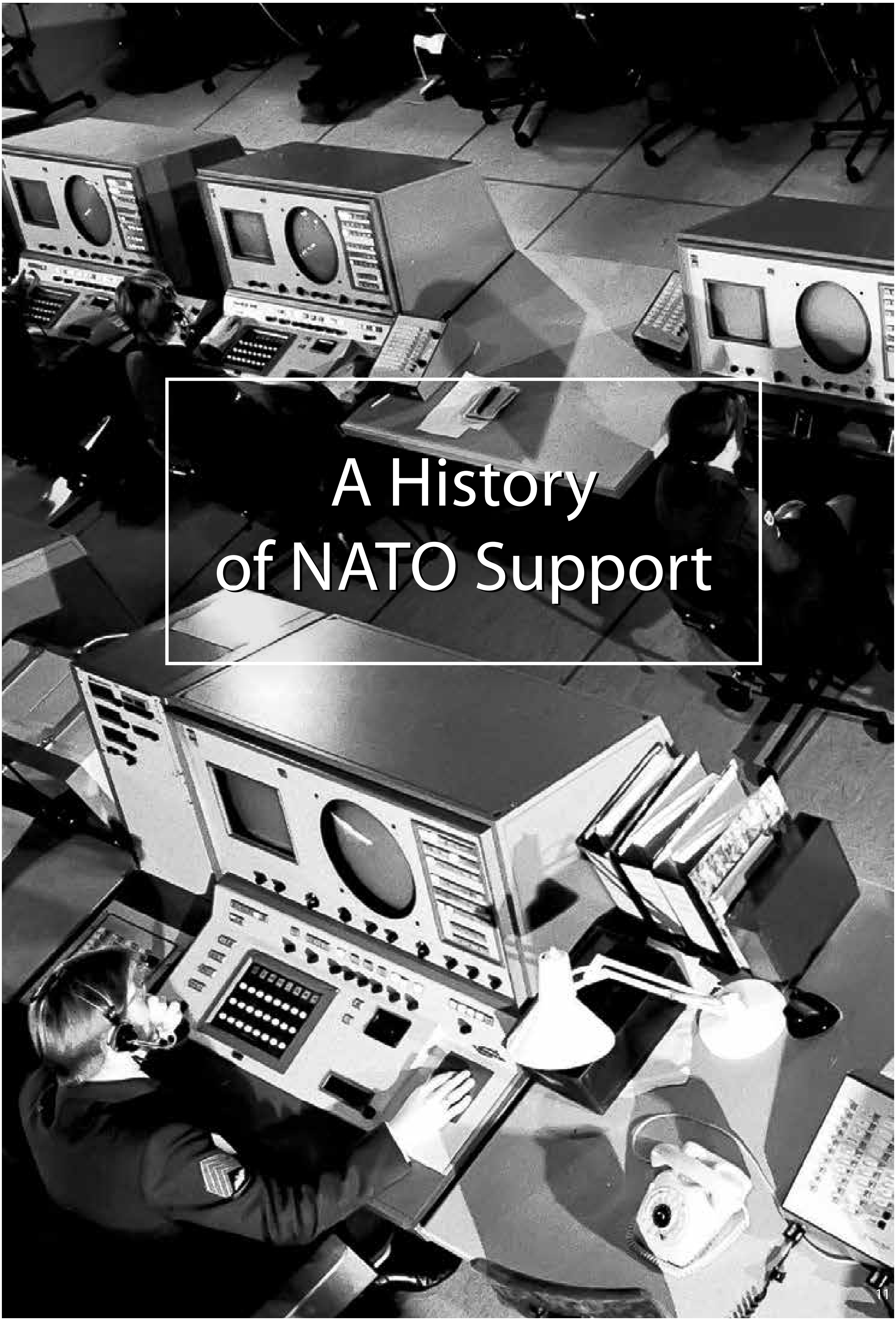
Quantum sensing

Quantum technologies in sensing has huge potential, but is likely to have an impact beyond the three to five years window of our Technology Watch series. However quantum radar, and new mechanisms to sense minute changes in gravity, electric field or magnetism have the potential to detect hidden massive objects (machinery and weapons), or movement of people beyond the line of sight, for example in the urban canyons of a modern city environment. Quantum sensing could make our oceans essentially transparent.

Quantum radars exploit entanglement and can significantly enhance target detection capabilities. These systems rely on entangled photons – the elementary particles of the electromagnetic field. As such, quantum radars offer a significant improvement in performance and the possibility of detecting and identifying stealth targets. Also, they are more resilient against the use of jamming countermeasures.

Quantum technology is now firmly into the realm of science fact rather than fiction, as it is providing (or promising) a step-change in the technological capabilities of C4ISR systems – and those of our adversaries.

By Peter Lenk and Michael Street,
Service Strategy



A History of NATO Support

We’re 5!

Compared to NATO’s nearly seven decades in existence, the NCI Agency seems very young, having been established on 1 July 2012. But our roots reach as far back as 1951 and we should be proud of our DNA. This year’s special anniversary is an opportunity to take an express ride through the rich history that make us who we are today.

Always at the soldier’s side

1995 was a special Christmas. For the citizens of Sarajevo, it meant being able to walk to get water without being shot. For NATO, it marked the start of the first peacekeeping operation of the Alliance since its creation, a significant departure from its previous missions.

On 20 December 1995, NATO, an organization designed to protect a well-defined territory from members of the defunct Warsaw Pact, was put in charge of leading a force of over 50,000 troops from 32 countries to enforce peace accords. The Alliance’s top commander at the time otherwise known as Supreme Allied Commander Europe (SACEUR), US General George Joulwan, considered it critical for the troops to arrive swiftly in unison, in what would be a powerful ‘show of force’.

“It was clear to me that if we did not show strength at the outset, parties opposed to the peace, snipers, might be tempted to attack our forces, trying to weaken our resolve,” he reflected several years later.

The historic deployment included Russian peacekeepers, who had until then only ever practiced how to maneuver against – not with – NATO. Logistics were further complicated by the harsh winter and an infrastructure decimated by conflict and the heavy use of landmines.

General Joulwan turned to a precious resource, the SHAPE Technical Centre (STC) in the Netherlands. Established in 1955 as the SHAPE Air Defence Technical Centre (SADTC), it was responsible for providing technical advice to the operational community. The team proposed leveraging advanced software to plan, stage and execute troop movements. It worked so well, that SACEUR invited CNN to visit the offices in The Hague, proudly saying: *“I could not have done Bosnia without the SHAPE Technical Centre,”* he added.

“We are pushing the envelope but it’s working. Even in the worst part of the year, and the worst part of Europe to deploy a force, it’s very reassuring to know what you [the Shape Technical Centre] have done.”

What started in Bosnia continued; the NCI Agency’s predecessors went on to support NATO’s Kosovo Force (KFOR) after the Alliance received its mandate from the United Nations in June 1999.

Two years later, our technology allowed NATO’s AWACS radar aircraft to patrol the skies in the US, contributing to the Alliance’s first anti-terror operation. The Agency’s expertise extended to creating a mission operations centre for NATO in Afghanistan, and improving the commander’s situational awareness off the coast of Somalia as part of a counter-piracy operation. And then, there were special missions. For example, when NATO airlifted African Union peacekeepers to Darfur in Sudan, in a bid to end the violence there.

By then, NATO’s technical community had grown (see chart next page). But what did not change was the fact that our technicians were in lock-step with NATO’s soldiers, sailors, airmen and women.

“Whether the mud of Kosovo, the searing heat of Somalia, the story of NATO operations is also our story, the technical community being there side by side with the soldiers, frequently first in and last out,” said Bernd Kremer , Chief of Network Services and IT Infrastructure at the NCI Agency.

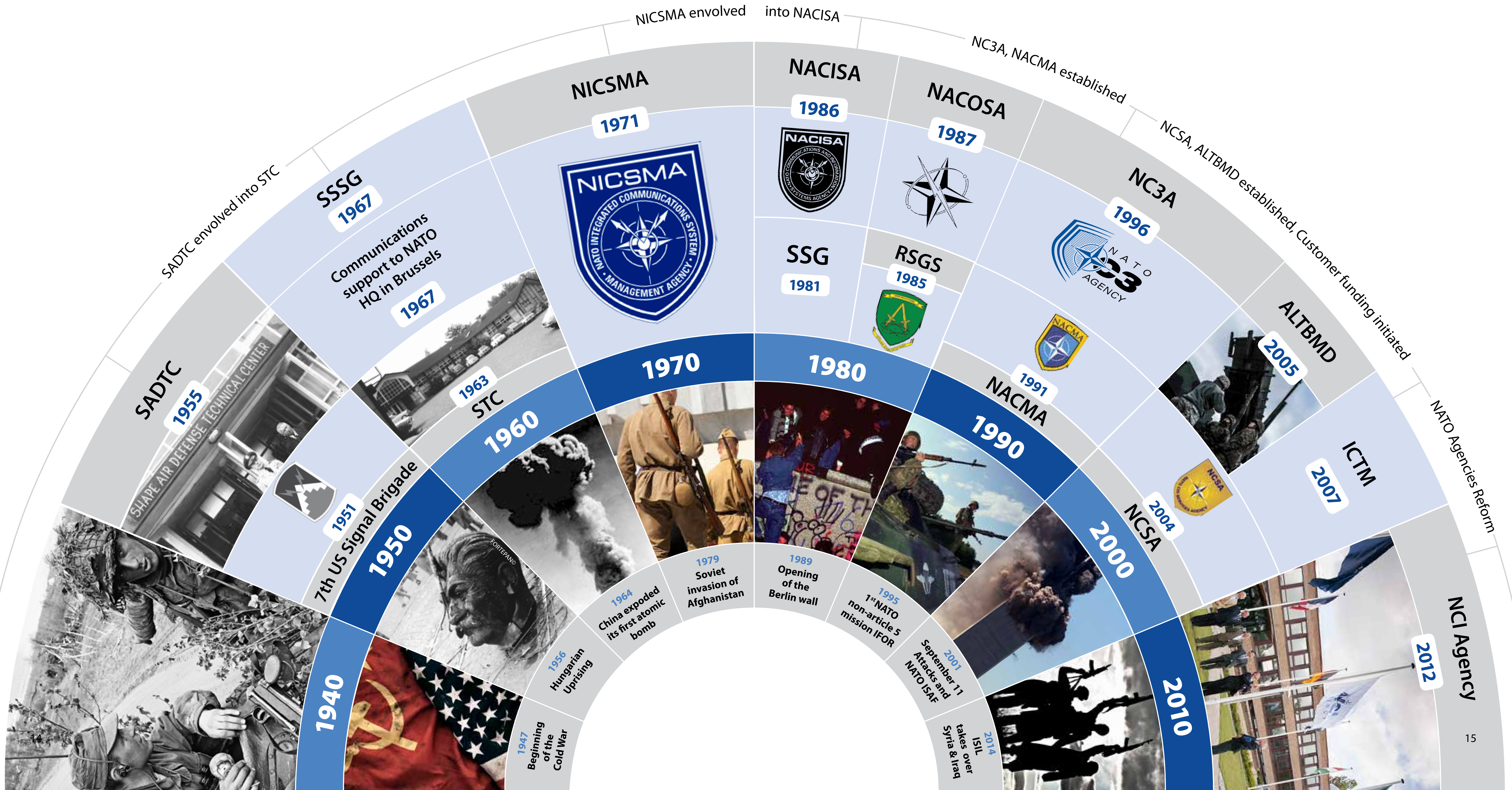
“I think this is an important element that our customers should remember. We were with you on all those operations, that knowledge helps us be ready for the next challenge.”

Breaking the rules

“Yesterday six people died, I need you to fix secure voice now,” said General McChrystal in Afghanistan, speaking at an urgent meeting

SADTC	SHAPE Air Defence Technical Center
STC	SHAPE Technical Center
SSSG	SHAPE Signal Support Group
NICSMA	NATO Integrated Communications Systems Management Agency
SSG	Service Support Group
RSGS	Regional Signal Group SHAPE

NACISA	NATO Communications and Information Systems Agency
NACOSA	NATO CIS Operating and Support Agency
NACMA	NATO ACCS Management Agency
NC3A	NATO Consultation, Command and Control Agency
NCSA	NATO CIS Services Agency
ALTBMD	NATO Active Layered Theatre Ballistic Missile Defence
ICTM	Information Communications and Technology Management



SADTC envolved into STC

NICSMA envolved into NACISA

NC3A, NACMA established

NCSA, ALTBMD established, Customer funding initiated

NATO Agencies Reform

SADTC 1955

7th US Signal Brigade 1951

STC 1963

SSSG 1967

Communications support to NATO HQ in Brussels 1967

NICSMA 1971

NACISA 1986

SSG 1981

RSGS 1985

NACOSA 1987

NACMA 1991

NC3A 1996

NCSA 2004

ALTBMD 2005

ICTM 2007

NCI Agency 2012

1940

1950

1960

1970

1980

1990

2000

2010

1947 Beginning of the Cold War

1956 Hungarian Uprising

1964 China expoded its first atomic bomb

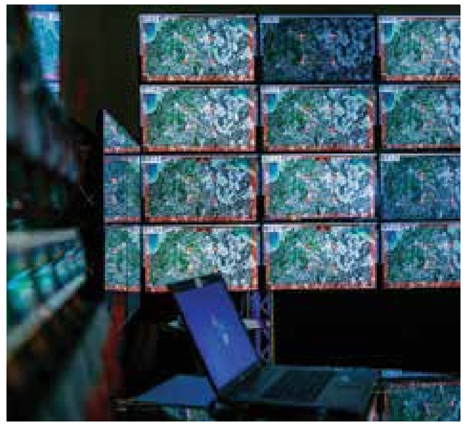
1979 Soviet invasion of Afghanistan

1989 Opening of the Berlin wall

1995 1st NATO non-article 5 mission IFOR

2001 September 11 Attacks and NATO ISAF

2014 ISIL takes over Syria & Iraq



to representatives of two organizations: the NATO Communications and Information Agency (NCSA) and the NATO Consultation, Command and Control Agency (NC3A).

The Commander of US and ISAF forces in Afghanistan was speaking in the middle of an intense counter-insurgency campaign which relied heavily on CIS to be successful.

This sense of urgency, driven by the dangers facing military staff every day, precipitated technological breakthroughs for the Alliance time and again.

"When you are working on the ground with the operator, the tempo is different, you are constantly pushing the envelope. Sometimes it's never been done before, and then you simply have to be creative to satisfy the operational needs for the sake of the soldier in the field," said Detlef Janezic, Chief of Service Engineering and Architecture at the NCI Agency.

In the early 1990s for example, NC3A and NCSA introduced for the first time a network for secure email and data exchange between headquarters, while the rest of the world was still predominantly using insecure faxes to transmit important information.

This secret network, first called 'Echo' and later 'Cronos', revolutionized military communications. It provided a resilient planning tool, and gave commanders vital and rapid situational awareness.

It also inspired the creation of a mission network, later evolving into a federated mission network concept, which today ensures the interoperability of NATO and non-NATO forces in multinational operations. Operation Joint Endeavour in Bosnia was not the only catalyst for technology leaps, the NATO-led International Security Assistance Force (ISAF) mission in Afghanistan also raised many challenges which could only be overcome thanks to the expertise of the Agency's talented staff.

In 2007, the Allied Rapid Reaction Corps notably started using chat prototypes which had been developed by Agency scientists to support critical, time-sensitive tasks such as medical evacuations.

This allowed medical staff in theatres to report casualties and evacuate them more quickly, saving hundreds of lives in the process.

"Our history is a history of 'firsts'," added Mr Janezic, *"Driven by operational demands, sometimes by the pace of technology, we often have been stretching the rules in terms of what can be done. That has sometimes made us not too popular with the Committees."*

Part of this journey was close partnership with Industry, and pushing the boundaries of that partnership.

From 2007, the Agency outsourced part of core CIS services for the ISAF mission to Industry. This marked the start of a new type of symbiotic relationship between the organization and the private sector, with Industry providing IT support to NATO forces, while the Agency focused on complex, interoperability work.

Two years later, a contracted Industry partner went on to establish ISAF Joint Command in Kabul under our direction, turning a social centre with a gym into a fully-fledged, secure operations centre within weeks.

People – at the heart of technology

There's only so much technology in our story. First, not all our work is about technology, one of the Agency's key assets is a team of operational analysts that provide everything from analytical support to deployed forces and analyses of a mission's progress, to more unusual work such as the development of a fog dispersal machine which was trialled at Sarajevo airport.

But there is also an important wider point. *"We are not about factories or robots. Every challenge has come down to a group of people deciding to do something about a problem,"* stressed Mr Janezic.

"It's the human network that makes NATO strong. Partnership with Industry and Nations is key," said Michael Stoltz, Acting Director of Air Command and Control (AirC2) Programme Office at the NCI Agency.

NACMA, the Agency which was established to manage NATO's air command and control system (ACCS), is another founding member of the NCI Agency. Worth over 2 billion EUR, ACCS is one of NATO's largest technology programmes to date and it will soon be playing a key role in NATO's Ballistic Missile Defence. The system combines the planning, tasking, and execution of all air operations both over NATO European territory and out of area when deployed.

When fully rolled-out, ACCS will interconnect more than 20 military aircraft control centres, increasing the effectiveness of NATO air operations and covering 10 million square kilometres of airspace.

"Air defence is a classic example where the Nations can do more together than most Nations can do alone," Mr Stoltz added. *"The technology landscape evolves, and at the core of being able to respond to this evolving landscape is close connection to the operational community, dialogue with the Nations."*

Today, the Agency's various locations host over 20,000 visitors a year with discussions ranging from standards on information-sharing to evolving doctrine and cyber innovation.

"What is impressive to see is what a determined group of individuals can do. Soon, NATO's Alliance Ground Surveillance fleet of Global Hawks will take to the skies, providing the Ambassadors with unparalleled additional information.

The basis for the data information-sharing started as a group of nine Nations who worked with the technical community to drive forward standards, which have now been adopted in NATO," said Joe Ross, Principal Scientist of the Agency's Intelligence, Surveillance and Reconnaissance team.

Similar multinational projects have changed the face of NATO cyber cooperation and relations with Industry.

In the wake of the 2014 Wales Summit for example, the Alliance launched the NATO-Industry Cyber Partnership (NICP), which now boasts 12 information-sharing agreements between Industry and NATO.

"The trust we have built through this programme has proved essential during incident response, resulting in faster communications and sharing of more contextual information that bolsters our collective cyber defences," stressed Ian West, NCI Agency, Chief Cyber Security, *"That human network is precious."*

Another Christmas, another challenge

The NCI Agency flag was first raised on 1 July 2012 in Kabul. It was a Sunday but a normal working day in Afghanistan and perhaps a symbol of our enduring commitment to operations.

Shortly after the Agency was established came another Christmas challenge. The conflict in Syria was escalating and cities in nearby Turkey came under threat of Scud missile attacks. The Netherlands, Germany and The United States offered Patriot batteries to augment Turkey's air defences.

The Agency had two weeks over Christmas to connect these Patriot batteries to NATO's command and control networks and the Alliance's air commander in Ramstein, Germany. In one of the cities, 3 million people were at risk.

"There is something about Christmases in NATO," said Alessandro Pera, the head of the missile defence programme at the time, *"There is frequently a present in the form of a mission."*

The connection was done on time, leveraging the first ever operational use of cloud computing to reduce the amount of hardware (and therefore logistics) needed, giving SACEUR the speed of response he needed. Given the sensitivity, this time there was no CNN visit.

NATO today is very different from the Alliance in 1955 or 1995. So is the technology community. In 2012, five key pillars of that community merged into one.

But just like the Alliance's fundamental values have endured, the core of what made NATO's Supreme Allied Commander Europe so proud in 1995 has not changed – a group of talented people determined to rise to any challenge in support of NATO's soldiers, sailors and airmen and women.

By Michal Olejarnik, Chief Strategy Office

CONNECTED TODAY

FOR THE PARTNERSHIP OF TOMORROW

Nurturing NATO's transatlantic bond might never have been as important as it is today. With the US administration re-positioning itself on the geopolitical stage, and a growing number of threats such as cyber and terrorist attacks affecting North America and Europe equally, the Alliance needs to stand united.

The NCI Agency's CIS Support Unit in Norfolk, Virginia helps reinforce the transatlantic bond by ensuring that Allied Command Transformation (ACT), NATO's headquarters in the United States, is connected to its overseas counterparts at all times.

Norfolk is one of three locations (apart from Mons and Brussels in Belgium) where the Agency has also established a Strategic Partnership Office. The small office, which represents the Agency in the political arena of ACT, works alongside the local CIS Support Unit (CSU) staff to provide a coherent Agency presence for North America.

The American headquarters, driving transformation

ACT is one of two Strategic Commands in NATO, the other being Allied Command Operations, located in Mons, Belgium. ACT promotes and leads many initiatives designed to transform NATO's military structure, its forces, capabilities and doctrine. Allied Command Transformation's main responsibilities include education, training and exercises, as well as conducting experiments to assess new concepts, and promote interoperability throughout the Alliance. ACT is the only permanent NATO headquarters outside of Europe and the sole NATO headquarters in North America.

Multitude of customers

While CSU Norfolk is recognized for supporting ACT, an often overlooked fact is that the unit also provides capabilities to a host of external customers. "*The biggest misconception is that CSU Norfolk's sole purpose is to support the ACT Headquarters. Although, this is a major part of the workload, the unit is also the Agency's technical footprint in North America. We provide support to a multitude of national customers in the US and Canada,*" said Phil May, Head of Infrastructure Management at CSU Norfolk.

What is a CSU?

CIS Support Units (CSU) are small divisions made up mostly of technical experts. Their mission is to provide Information, Communications and Technology (ICT) services to the assigned NATO unit, uninterrupted and of a high standard. This means, they are located all over the Alliance, from Norfolk, US, through Lisbon, Portugal, to Stavanger, Norway. They make sure that NCI Agency's NATO customers have technical representation at their location, at all times.

The unit's support to ACT ranges from providing subject matter expertise and creating safe environments for innovation and experimentation, to its cyber team providing expert guidance on cyber security threats, trends and initiatives.

However, the CSU's role does not stop there. It has an important part to play in North America's busy military calendar: it connects participants and locations during exercises. In this, the unit has a reach beyond ACT Headquarters and provides vital support to 19 US and seven Canadian elements ensuring their connection to NATO, including extensive support to the US Navy fleet during training and exercises.

A strategic link

Utilizing its geographic location alongside ACT and key national and multinational entities in North America, the American Strategic Partnership Office provides the Agency's unique perspective on transformational activities affecting the Alliance, like enhanced education, interoperability and future challenges.

What is a Strategic Partnership Office?

The Strategic Partnership Offices provide a bi-directional gateway to interact between supplier and customer. From a formal Strategic Partnership perspective, they are responsible for relationship management; an enduring, day-to-day process to manage expectations, facilitating conflict resolution, and representing the Agency's interests. More broadly, they provide a 'one-stop' NCI Agency presence dedicated for each of the customer groups and act as a trusted advocate for both supplier and customer.

Reinforcing the Agency's presence with a small Strategic Partnership cell in Brussels and at the two Strategic Commands is an indication of how important it is to sustain and further develop relationships with these key partners. While the CSU is making sure that ACT's day-to-day business runs flawlessly, the Strategic Partnership Office looks ahead to inform current and future decisions. "*We are an intelligence gateway between the Agency and the Command, a strategic representation of the Agency in NATO's US headquarters.*" says Strategic Partnership Officer Virginie Viscardy. "*From enhanced education, training, and exercises programmes, to engaging with ACT senior leadership, essentially representing the Agency's General Manager, we are responsible for reinforcing the transatlantic bond through close cooperation.*"

Connecting transformation

The NCI Agency's Norfolk staff not only makes sure that the Transatlantic Command is connected to Europe and to other partners via cables and through routers with the support of CSU Norfolk, but on the strategic level as well, thanks to the relentless work of the Strategic Partnership Office. Driving NATO transformation is a complex task. Being online and connected is the first step to do it well.

Written by Livia Majercsik, Chief Strategy Office
and Robert Hyatt, Senior Enlisted Advisor

Strength in numbers:
Supporting the Afghan mission

"Final destination, Kabul!" exclaimed the startled airport official, and with that, I found myself leaving the comforts of the Netherlands for the unknowns of Afghanistan.

Shortly after starting at the NCI Agency, I heard about the possibility to deploy to the NATO Resolute Support Headquarters and work as an analyst within the Afghan Assessment Group (AAG). I was immediately keen to get involved.

I figured deploying to Afghanistan would be a unique opportunity to gain first-hand experience of NATO operations, work closely alongside military and civilian colleagues from around the world, and be part of the broader effort to train, advise and assist the Afghan security forces and institutions.

Boarding the plane at Schiphol in early April, I was very excited about this new challenge, but also unsure of what to expect when landing at Kabul Airport the following day.

The team I worked with, the AAG, is responsible for campaign assessments of the Resolute Support mission. This includes analyzing progress towards achieving campaign objectives, and improving the way operational data feeds into the commander's situational awareness by applying both quantitative and qualitative techniques.

Since 2011, the Operational Analysis (OA) Service Line (SL) has provided year-round support to this group, through both a deployed analyst on a two-month rotational basis, and also analytical reach-back support from analysts in The Hague, Netherlands. The OA SL analysts provide not only specific technical skills such as expertise in programming and statistics, but also a wealth of experience and 'corporate knowledge' gained through years of experience supporting the Resolute Support and ISAF (International Security Assistance Force) missions.

Some of the products provided by the AAG are only distributed within the Resolute Support mission but some analysis, such as the Periodic Mission Review, makes it all the way to national governments to inform their policy on Afghanistan.

Life at Resolute Support Headquarters is surprisingly comfortable and varied considering the compound only measures around 1sqkm. Everything is within quick walking distance. There are plenty of amenities including an Italian café, a Turkish and a Thai restaurant and a variety of shops and markets selling everything from authentic carpets, lapis lazuli stones and paintings by local artists. Every Friday, the headquarters welcomes a number of local traders into the camp for a 'bazaar' selling even more Afghan wares. This contributes to a source of income for the Afghans working there.

With an American friend, it's also possible to head over to the US embassy next door to catch a recently-released movie in their cinema and even enjoy some freshly-made popcorn. The atmosphere on camp is generally very friendly and welcoming given that everyone is away from their friends and family, with military and civilians working together throughout nearly all departments. Our group held a weekly board game and pizza social night, with prizes awarded to the most successful gamer at the end of the month. This was a great way to relax with colleagues after a long working day. Every so often, the updates and sounds from outside the green zone, accompanied by the various alarms and klaxons provided a stark reminder of the situation on the other side of the huge concrete walls and the dangerous reality that the locals face.

As well as the analytical day job, we were fortunate to be involved in the mission's Train, Advise and Assist efforts (TAA) which is one of the most fulfilling elements of any deployment to Afghanistan. Every week, we headed over to the Afghan Ministry of Defence (MOD) and provided training to the Plans and Strategy staff in Operations Assessment, Analysis and Data Visualization.

A walk to the Afghan MOD, even though inside the 'green zone', required a full armed escort and we had to wear Personal Protective Equipment (PPE). But the trip provided a brief and rare glimpse of life outside the compound. As most of the Afghan military don't speak English, teaching was done through an interpreter. This brought a whole new level of difficulty to the task, and a 30-minute lesson could sometimes take over an hour. However, it was a great opportunity to meet and talk to members of the Afghan National Defence and Security Forces, who will be so vitally important to the country's future. It was also an excellent reminder of the purpose of the NATO mission there.

Despite the longer working hours, and seven-day working weeks, time flew by in Kabul thanks to the interesting work, experiences and people from all over the world that I was lucky to meet!

by Nicholas Labsvirs,
Operational Analysis Service Line

Conversation with Kevin Scheid

On his career to date and his plans for the NCI Agency as the new General Manager.

"How old were you when you got into the White House?" I ask the NCI Agency's new General Manager, not unimpressed by his extensive CV.

*"12,"*he replies deadpan, not even a hint of a smile on his face to give away his obvious wit.

We're halfway through the interview, and Kevin Scheid hasn't missed a beat. Quick on his feet yet careful with his words, he is not one to be caught off guard.

But as he takes up his new role, the Pennsylvanian native agreed to chat with the Communicator to reveal how he ended up in the hot seat, and his future plans for NATO's cyber and tech arm.

Taking measure

So is the NATO Communications and Information (NCI) Agency headed for a radical makeover with its first American national at the reins?

"I plan to take the first 90 days, like most new heads of large organizations, and do some deep-dives in some key areas, to make sure I understand the status and state of the Agency…

First, I'll hold deep dives in the areas of finance and the customer-funded regime, personnel management and the contract issues and how that is progressing, in acquisition, as well as the management of the organization. Do we have the right management structure for the Agency? Following that, I'll do the same for major programmes and projects.

And then, what I also want to do is put together a small transition team to help me get an independent, objective look at how the Agency has evolved over the past five years.

This team will be made up of people from inside and from outside the Agency, as well as some consultants that have particular skills - a small group. For six to eight weeks, they will dig into the same issues that I will be looking into and then give me their independent views on them."

Kevin Scheid is not exactly new to NATO. Between 2009 and 2012, he held the joint titles of Deputy General Manager, Chief Operating Officer and Director of Acquisition of one the Agency's predecessors, the NATO Consultation Command and Control Agency (NC3A).

He may have left The Hague five years ago, but his work with the MITRE Corporation – which he describes as an organization with *"a similar model to the Agency but with much more overhead funding"* – and his recent stint overseeing the new NATO Headquarters IT programmes, have given him more than a good understanding of how things stand.

Setting objectives

"I don't believe you can delegate strategy and I don't think you can delegate change management.

So in the first 90 days I want to put together a new strategy with the Agency Supervisory Board (ASB), with the Directors, and with the Agency at large.

After my deep dives into the Agency functions, I will work with the ASB to develop a five-page strategy with goals and objectives that we can realize over the next three years."

Why five pages only? *"Brevity is key – you need to have that."*

He may also have been inspired by another American civil servant, Robert Gates, the former US Secretary of Defense.

"There is an example where Bob Gates, who was then the Deputy National Security Advisor to General Scowcroft, wrote a memo which came out on the day of [Bush Snr's] inauguration to set up the whole structure for the National Security Council process.

It was five pages and it covered all the contingencies, all the various committees etc. And from that day forward, it never changed.

That is the difference that experience in public policy makes, because they know exactly what they want. They know this because they have seen before what worked and what didn't work."

Scheid could easily argue that he has also seen what works and what can be improved after his 32 years serving in the US government. He spent 11 years at the White House Office of Management and Budget, supporting three administrations, before working with the US Intelligence Community for a decade. After the September 11 terrorist attacks, he was asked to serve as a senior Team Lead on the 9/11 Commission, which made recommendations on reforms of US intelligence.

Most recently, he served in the US Department of Defense in the positions of Deputy Comptroller and later as the Assistant Deputy Chief Management Officer within the Office of the Secretary of Defense.

Doing the maths

"As a budget examiner for the Office of Management and Budget, you learn to ask tough questions and gain quick insights into federal programs. I then had the pleasure of working with the US intelligence community where I had oversight of large, multi-billion dollar programmes. Sometimes I didn't do well, sometimes I did. I've learned a lot over the years.

I was the Deputy Comptroller of the Department of Defense at a time when NATO was engaged in Afghanistan and the US was engaged in Afghanistan and Iraq, both going simultaneously, so the US would spend 500 billion USD just running the military and then we spent an additional 160 billion USD annually at the peak of the two wars. So we were spending nearly 700 billion USD a year on those efforts."

The NCI Agency has a budget of roughly 1 billion EUR a year, how can that even come close to comparing with the previous figures Scheid has had to juggle?

"The skills are still the same, and I don't mean to be trite, but the zeros don't make a difference to me.

The NATO Nations are careful with the money they invest in these projects, so every Euro is important, every Euro is dear and we have to get the most out of it. And I think it's one of the big challenges in this job. How do we work to help secure Europe with the resources that we have?

As the Nations invest more in defence, how can NATO and the NCI Agency play a thought-leadership role in guiding some of those investments?

Because if we work together as we collectively invest, there is a multiplier effect in the way we can spend the money."

The NCI Agency's top man has always had a good head for numbers. Well before he was responsible for national and organizational budgets, Scheid worked hard to put himself through college.

"I actually worked for four years after high school. It was essentially because of finances. In the US, you pay for college, it is not subsidized to the same extent as in Europe so students and their families pick up most of the bill.

My family lived outside of Chicago when I finished high school. I worked the first few years in a Marriott hotel there, and then eventually I moved to Austin where I had family and took a job in an IBM factory, building typewriters. And just down the street from my student apartment was a dormitory where a young man named Michael Dell was living.

Dell started building computers in his dorm room and now that whole area where the IBM factory was is all Dell factories. He's had a very different career path than I…"

Scheid took up to three part time jobs to finance his Undergraduate Degree in Economics and later his Graduate Degree at the Lyndon B Johnson School of Public Affairs, at the University of Texas.

"I managed the apartment building I lived in for the owner. And I was a computer operator which distantly ties to what I am doing now."

Serving the public

Like Dell, he could have started his own company, so why aim for the White House?

"I have always been inspired and moved by public service, I enjoy it and I don't get the same psychic benefits from corporate work.

That's why, although at the time I wasn't driven by public service, I entered the LBJ School of Public Affairs, because they had a very good international programme.

And I had an opportunity while in graduate school to work under an excellent professor who was focused on international trade and defence issues… He helped me get an internship working at the US embassy in Thailand.

Thailand at the time was immersed in security issues related to Cambodia and the Thais had requested the purchase of a squadron of F16 [fighter aircraft] from the US. The question the ambassador had for me during my internship was: 'If they buy this, what is the impact on the economic development for Thailand? What is the impact on the population?' So I did some economic analysis and that got me initially interested in defence issues."

Shortly after completing his internship, Scheid fulfilled his ambition of getting a job in Washington, and within three years, he was back working on defence issues. One might wonder why he didn't stay at the Pentagon given his attachment to public service and his obvious dedication to his country.

"The Department of Defense is a very large and complex organization and there are lots of excellent people there. Here at NATO I have found not only excellent people, but a challenging environment due to its international aspects.

I am a strong believer in NATO and I am a strong believer in getting the Nations at the table to work through their problems.

For NATO to be successful, you need all its entities to work well together, and once you have this, you can really change the world.

And that's not a trite conversation or point. Look at the work NATO has done in Afghanistan, look at the work it has done in the Balkans, look at the work it is doing right now in the Baltics just to preserve the peace and to project stability. I think NATO has a great mission and the NCI Agency has a great mission within NATO."

Staying the course

Scheid plans to stay "annoying close" to the Agency's three main locations – Brussels and Mons, in Belgium and The Hague, in the Netherlands – in the coming year to keep project delivery under control.

"This is part of what I'll be looking at during the deep dives. What is the performance of our projects and programmes? Where do they stand? Are we doing everything we can to deliver on time and on budget?"

But he also intends to regularly meet with the Agency's 30+ CIS Support Units (CSUs) across NATO, as they are an "*integral and critical*" part of the Agency.

Given his transatlantic connection, he intends to build closer ties with Allied Command Transformation in Norfolk, Virginia, and with the US and Canadian governments.

"I just want to make sure we cover North America and we also need to find a structured way of engaging with other governments on a regular basis."

He has already set out big expectations and it is also clear that the Agency's new boss is a man of strong principles.

"When I was 11 years old, I gave up meat and it scared my parents, they didn't know what was going on." He may have been a schoolboy at the time, but he was already determined. And so, he stuck to his decision.

"Then as an adult I realized I simply don't like meat and I don't need to eat it with all the options we have now with fish and vegetarian dishes."

As people acquire more responsibility, maintaining a good work/life balance becomes more difficult. Health is often the first casualty of a thriving career.

Reaching new heights together

"I do not have particularly good habits. I enjoy working, I am single, I don't have a family and I am a bit obsessive at work which is not healthy.

Knowing that, I am trying to get some balance by exercising a lot and that's where I got into mountaineering and climbing a few years ago. And the climbing is less important than the months of training that lead up to it and that's where it pays off health-wise.

As I hit some critical birthdays, it sort of reminded me I needed to take care of myself. Mountaineering is tough on the body, I've had altitude sickness a few times. It's a real personal challenge.

All you're doing is putting one foot in front of another. It's very simple in principle but it's very complicated when you try to climb at higher altitudes. And there's nothing gray about it, it's either black or white. You train and you train and you prepare, and you either make it or you don't.

I like that clarity about it, because there is only one spot at the top, so you work to get to the top. There's not a lot of clarity in modern life, but with climbing it is clear. Climbing is also a team sport. At higher altitudes, you are roped to your team members and you either work together or you fail."

Unsurprisingly, his attitude to sport is not far off his attitude to business.

"They're dependent on you, you're dependent on them and you have to work together as a team…

A lot of what we do with the Agency, a lot of what we do in business to achieve big things, means working as a team."

So while he may be permanently assessing the situation and the people in front of him, and he may ask some tough questions, Scheid really is a team-player.

"I want to walk the halls and meet people on the first day. I want to engage with people directly so that they know they can talk to the General Manager, and the General Manager hears what they are saying, knows what they are doing and that there is connection there."

So be ready for that knock on your door because Scheid intends to move mountains with your help.

By Adelina Campos de Carvalho, Creative Media Centre

BALTOPS

a NATO maritime exercise with 46 years of history

Maritime cooperation in the East

The Eastern border of NATO has received considerable reinforcement in the past year not only with the creation of the NATO Force Integration Units (NFIUs), the Alliance's small headquarters in eight countries, but also with the establishment of an enhanced Forward Presence in four of these eight Nations.

Baltic Operations (BALTOPS), an Allied maritime exercise taking place in the Baltic Sea might seem like an extension of that undercurrent, but in fact, it is one of NATO's longest-standing exercises, having been conducted since 1971.

Originally, BALTOPS was exclusive to NATO Member Countries. But since 1993, Partner Nations have also been invited to participate, extending BALTOPS to Partnership for Peace (PfP) efforts, focusing on joint maritime activities, with particular emphasis on submarine search and combat, mine warfare, air defence, and maritime missions.

Every year, the exercise is conducted by a different host. This year, the NATO Naval Striking and Support Forces (STRIKFORNATO) took on the mantle.

STRIKFORNATO is a rapidly deployable maritime headquarters, which provides scalable command and control for the Alliance. This organization which is managed under a Memorandum of Understanding, has a rich history. When it was created in late 1952, six Member Nations contributed to its personnel and it only operated in southern Europe. It now covers the entire NATO Area of Responsibility and comprises 12 Member Nations.

Connected at Sea

Carrying out such a large scale exercise requires a great deal of coordination, preparatory work, and state-of-the-art connectivity. As with most NATO training exercises, the NCI Agency played a key supportive role before and during BALTOPS. The Agency's CIS Support Unit (CSU) in Lisbon was the main point-of-contact for BALTOPS17, starting preparations early in the year by attending the exercise's main planning conference in Vilnius, Lithuania in February.

Although, the Agency only delivers a small portion of BALTOPS' IT requirements, its role is important. It provides secure communications to one of the two flagships taking part in the exercise, HDSM ABSALON, a Danish frigate-sized support ship. The CSU also supports the Exercise Control element located ashore in Glücksburg, Germany. Despite the name of the exercise, Agency staff are not present physically anywhere near the Baltic Sea. Routing and connecting is done from the Agency's technical centres in Mons, Belgium, and in The Hague, Netherlands.

Coordination and collaboration

BALTOPS is always a large scale exercise. This year, 14 Nations participed with about 5000 troops, 50 ships, and 50 fighter aircraft and helicopters in the southern and middle Baltic. Many of the countries with a coastline on the Baltic Sea served as the 'land component' of the exercise, so amphibious operations were conducted in Latvia, Germany, and Poland.

Given the number of Nations and NATO entities involved, BALTOPS remains one of the Alliance's most complex maritime exercise testing NATO's interoperability and the ability of its Member and Partner Nations to join forces at Sea.

By Livia Majercsik, Chief Strategy Office
and Lars Jaehrling, Operations and Exercises Service Line

Defence Innovation Challenge winners

Staying at the forefront of defence technology innovation is critical for the success of the Alliance. NATO must keep pace with emerging security threats in order to remain effective. For this reason, the NATO Communications and Information Agency holds annually a Defence Innovation Challenge, which fosters the creativity of small businesses and academia in areas of critical importance to the 29 Member Nations, such as C4ISR technology and cyber capabilities. This year, 48 proposals representing small and medium enterprises (SMEs) and academia from 12 Allies, were submitted for review to a panel of NATO experts.

The challenge's top 10 finishers showcased their proposals at the 2017 NCI Agency Conference and AFCEA TechNet International (NITEC17) that took place in Ottawa, Canada in April 2017.

The NCI Agency's former General Manager Koen Gijsbers commented: *"This challenge affirms that the cutting edge technology we need to stay ahead of emerging threats is out there, and we are committed to finding innovative ways to connect with the small businesses and academic institutions that lack visibility within NATO but have much to offer the Alliance".*

Aditerna GmbH (Germany)

An online platform to share and execute models and simulations as a service

Focus Area: Rapidly deployable, scalable IT infrastructure

Aditerna GmbH developed aditerna SRP, an online platform to share and execute models and simulations as a service. It supports the entire simulation lifecycle, from model development to professional training and exercise management for industrial and military users.

Alessandro Busachi – Cranfield University (United Kingdom) and Babcock International

Optimizing applications of additive manufacturing in defence support services

Focus Area: Rapidly deployable, scalable IT infrastructure

Alessandro Busachi's work looked at modelling the applications of Additive Manufacturing in the context of Defence Support Services to reduce the reliance of the Royal Navy on supply chains.

He has developed an Additive Manufacturing – Decision Support System (AM-DSS) software prototype to estimate and simulate Additive Manufacturing deployments for in-field manufacturing of spare parts.

Additive Manufacturing (AM) is regarded as an emerging and promising technology which could enable rapid, delocalized and flexible manufacturing providing strategic advantages to the Armed Forces.

Dencrypt A/S (Denmark)

Dynamic encryption for protecting smartphone conversations (Dencrypt Talk) and data links (Dencrypt Core)

Focus area: Rapidly deployable, scalable IT infrastructure

The Dencrypt Talk app for iPhone protects conversations with Dynamic Encryption (patent pending) directly between smartphones. The Dencrypt Server System may be installed and operated locally or used as a hosted service. Dencrypt Messages, File Transfer etc. is on the roadmap and Dencrypt Core may be implemented to add Dynamic Encryption to existing IT systems. The Danish Defence expects to accredit Dencrypt Talk for RESTRICTED use by late 2017.

iDelft BV (Netherlands)

Scalable eProcurement portal framework

Focus Area: eProcurement services

iDelft aims at improving the efficiency of the ordering process for bulk items and services by introducing scalable web portals. These portals will be based on the Open Source Drupal framework.

The core innovation is to run the various software components in so-called containers. By using Docker container technology in combination with Drupal open source software, iDelft achieves a rapidly deployable, scalable and reusable solution.

The intention is to create a number of eProcurement portals, each tailored for a particular organization or contract type.

Larus Technologies Corporation (Canada)

Total::Insight™ Decision Support System

Focus Area: Service management automation and analytics

Total::Insight™ is a multi-sensor, multi-source Decision Support System (DSS) for organizations such as NATO, developing mission-critical C4ISR systems.

It uses Computational Intelligence (CI), advanced learning techniques, prediction/assessment capabilities to combine/analyze the information from a variety of sources including passive and active sensors, existing trackers and correlators, and soft data (eg: weather or operator reports, web pages). This is all done in real-time, all the time.

OMX (Offset Market Exchange) Inc (Canada)

Industrial base data and economic impact analytics

Focus area: eProcurement services

The OMX platform is already an existing commercial technology. The system is an online procurement platform that allows large companies (such as Lockheed Martin, BAE and other international defence contractors) to send out procurement opportunities, manage responses, track and analyze supply chains and report on local spend in country.

The platform also has visualizations and powerful bid data and supply chain economic impact reporting.

This platform can be used to analyze the industrial base, survey for capabilities, compare technologies that exist within each country, post calls for innovation or calls for procurement requirements and track data on the supply base in ongoing programs.

The software platform itself is proprietary, but the data that is entered into the platform is always owned by its users.

Oxford BioChronometrics (United Kingdom)

Advanced detection of falsely-authenticated users via autonomous and remote-access trojans

Focus area: Cyber security, sensors, analytics, visualization

Maelström is an anti-malware Detect and Disrupt technology from Oxford BioChronometrics that can detect (currently undetectable) Remote Access Trojans, the weapon of choice for cyber criminals and state-sponsored cyber terrorism and warfare.

Radionor Communications (Norway)

Radio system based on phased array smart antenna technology

Focus Area: Long-range wireless communications; resilient, terrestrial long-range or rapidly deployable, scalable IT infrastructure

Radionor Communications supplies new generation tactical, high-capacity data links based on phased array antenna technology operating in NATO Band IV. This technology utilizes live video, location data and other sensors, and is intended for fast-moving vehicles, vessels and aircrafts.

Cordis Array is an IP-based adhoc tactical network that can form a mesh net, requiring no extra infrastructure.

The electronic phased array system operating at microwave frequencies with narrow antenna beams has a jamming robustness unmatched by conventional tactical data links.

SAAB Denmark (Denmark)

TactiCall multi-level secure voice for enhanced interoperability

Focus Area: Secure voice interoperability between multiple security classification levels

TactiCall allows operators to monitor a mix of secure (RED) and non-secure (BLACK) voice communications, and simultaneously be able to speak at either secure or non-secure level, as the situation requires. A unique feature is the ability to handle multi-level security, using rugged conventional IT technology and common criteria accredited security software by Saab Danmark.

SpyCloud (USA)

Protecting NATO from the use of non-public breached credentials

Focus Area: Cloud Security and Service Management Automation and Analytics

SpyCloud is a Breach Discovery and Alerting company headquartered in Austin, Texas. Utilizing proprietary tradecraft, SpyCloud recovers stolen and breached data from private sources at very high volumes. Up to 80% of the data that SpyCloud acquires is unique, cannot be found by scanners, scrapers or web crawlers, and is currently in the hands of threat actors. This platform alerts exposed customers well before normal breach notification timelines, improving their ability to mitigate harm against their most valued online assets.

For more information, please visit: www.ncia.nato.int/Industry/Pages/Small-and-Medium-Enterprises.aspx

by Industry Relations

NCI Academy

NATO breaks ground on C4ISR and cyber Academy

Portuguese Prime Minister António Costa, former NCI Agency General Manager Koen Gijsbers and top officials marked in May 2017, the start of construction of a prestigious NATO training facility in Oeiras, Portugal.

"We are breaking ground on the construction of an Academy that will be a pillar of a modern, future-ready NATO," said the former General Manager in his opening speech. *"The Academy will be a hub and incubator for Industry, academia and vendors involved in training technology."*

State-of-the-art facilities

The NCI Academy will provide expert training to civilian and military staff from NATO and its Member Countries on the Alliance's advanced IT and cyber systems, both software and hardware. Operators trained at the Academy will go on to man NATO's IT and communications systems, as well as its air, ballistic and cyber defences.

Not only will the subject matters taught at the Academy be cutting-edge, the facility itself will be state-of-the-art, with advanced technology connecting it to training locations in the Nations, Industry and academia.

Once fully operational, in the third quarter of 2019, it will replace several Agency training facilities, including the NATO Communications and Information Systems School in Latina, Italy, and the Air Command and Control Training School in Glons, Belgium.

A breathtaking location

Construction works, worth around 20 million EUR and funded entirely by NATO's Security Investment Programme (NSIP), are set to be completed in October 2018.

The public tender, approved by the Portuguese Council of Ministers in June 2016, was won by Mota-Engil, Engenharia e Construção SA, a major construction company in Portugal. The contract for the construction was then signed in March 2017 by the company and the Portuguese Ministry of Defence.

The contract foresees the construction of a 13,000sqm building. These facilities will be built within the scenic Compound Reduto Gomes Freire, in Oeiras, Portugal, the former home of Allied Joint Force Command Lisbon, which currently hosts NATO's Naval Striking and Support Forces, a detachment of the Alliance's Joint Analysis and Lessons Learned Centre and a national Portuguese command.

The building of the Academy is part of the overall process of streamlining NATO's IT facilities, launched in 2012.

By Education and Training Service Line

Defending a smart city:
Federating civil, military things and data

Internet of Things (IoT) technology has a huge potential for the military domain. Smart devices could help better protect NATO Member Nations, detecting threats more quickly, providing critical services to soldiers on the ground or even replacing them.

However, IoT was never envisaged for defence use. IoT security is a particular area where standard IoT devices don't meet typical defence security needs.

Rather than add military security to these small, cheap, off-the-shelf devices – turning them into large, expensive, custom-built devices – experts from the NCI Agency recently tested available IoT security mechanisms in their most robust modes. The demonstration took place at the International Conference on Military CIS (ICMICS) which brought together national research labs, NATO subject matter experts and Industry representatives in May 2017.

Michael Street, the NCI Agency's Service Strategy Innovation Manager said: *"Our aim was to show ways of exploiting the IoT to support military functions, while at the same time addressing technology challenges in the military use of IoT."*

The 'Things' in the Internet of Things typically use small microcontrollers with limited power consumption, limited processing and restrictions on their communication to the internet. This poses some challenges if you want to rely on them for something more critical than an IoT fridge ordering more milk. So we coupled traditional IoT security mechanisms with a number of other functions to increase resilience."

Hybrid situational awareness

The Agency team used IoT devices to which they added attribute-based encryption to protect data across the network, data analytics to determine whether the security of the device could still be trusted, as well as directional receivers to determine if the IoT devices had been moved or tampered with. They also worked with multiple sensor types and multiple networks to remove single points of vulnerability, and homomorphic encryption to allow partners to query encrypted data. The demonstration used a number of possible scenarios to explore the limits and potential of IoT in the military domain.

As part of these scenarios, IoT devices collected a combination of data from NATO, national and civilian sources. The data was then analyzed to improve hybrid situational awareness, using intelligence at the edge to fuse inputs from disparate cheap, consumer-grade sensors to form an accurate, resilient picture, and using big data analytics techniques to separate trustworthy and non-trustworthy sensor data.

"Information was harvested from both military and civil government IoT sensors. The former came from NATO and national military sensors, the latter coming from a number of local 'smart city' initiatives," Dr Street explained.

"Tapping into the data from smart cities provided additional situational awareness of the urban area, for example checking environmental monitors or traffic cameras. Using civil sources requires careful filtering to prevent information overload, and analysis for signs of interference or manipulation."

Smart, resilient societies

Data from NATO, Finnish, German and Polish IoT sensors was fused, filtered based on the geographic area of interest, and presented to commanders on a big screen in the simulated headquarters, and on a tablet in the simulated field. The tablet used the US Android Tactical Assault Kit (ATAK) to visualize data on a mobile device's common operating picture.

IoT is not only about sensing the environment. During the demonstration, once sensors were triggered by suspicious activity and data analytics deemed the incident worthy of investigation, a drone was deployed to the incident location. Artificial Intelligence on board the drone allowed it to navigate, track and classify objects autonomously. Meanwhile, a long-range, low power wireless platform (LoRa) communication module allowed the drone to report back to the headquarters over very long distances using low-power communications developed for IoT. Using Artificial Intelligence techniques at the edge reduces the bandwidth needed to communicate and the headquarters receives succinct information about the incident rather than a continuous stream that needs constant monitoring.

"The live demonstration highlighted the need for an architecture for the devices and data which can draw on the best elements from NATO and from the commercial IoT world," Dr Street went on.

"The demonstration went down so well that after the planned event it was repeated for the national members of the NATO Science and Technology Organization's Information Systems Technology Panel and for delegates at the Wireless Innovation Forum's European conference."

By Service Strategy

The International Conference on Military CIS brings together scientific, engineering, and military communities from across the Alliance and its Partners to share information on the opportunities and threats which technology is bringing to the military CIS environment.

Laying down the (cyber) law

As the recent ransomware attack WannaCry revealed, cyber-attacks are by nature invasive, and can affect every layer of society. As such, only a comprehensive response, involving experts from a wide range of fields, can be effective.

For this reason, every year, NATO, Allies and Partner Nations test their cyber resilience in the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. This exercise, which is organised by the NATO Cooperative Cyber Defence Centre of Excellence, not only tests the skills of cyber security experts, but also the support they receive from their legal teams, among other specialists.

In 2017 – and for the second year running – the NCI Agency's team won Locked Shields' legal challenge.

Cyber operations: a law unto themselves?

In order to defend against malicious cyber operations, organizations must rely on security experts who can immediately defend, deter and repair computer networks under attack. While skilled computer analysts might be able to identify what has happened and trace the attack, further steps cannot be taken without first consulting a lawyer.

The lawyer must analyze the applicable legal regime, and inform the cyber team of the boundaries of their actions. Making an assessment in a short timeframe can be challenging, especially in cyberspace as this requires on-the-spot interpretation of legal rules that were drafted a long time ago.

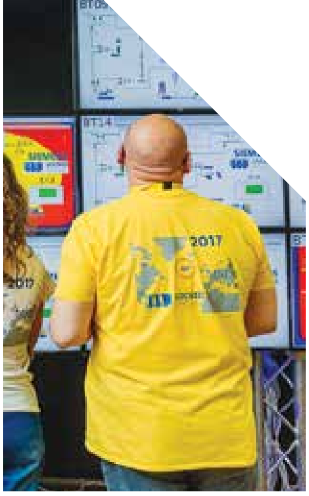
Depending on the nature and identity of the perpetrator, various legal remedies and frameworks may apply. In case of a local hacktivist group or a group of cyber criminals, legal remedies may involve a combination of international law enforcement measures and/or claims for damages in international private law.

However, if the malicious acts were perpetrated by a State, the victim State could invoke the 'law of State Responsibility' and seek remedies under international law.

Moreover, if the malicious cyber operation caused actual damage that amounted to a use of force by another State, it would possibly justify countermeasures or, ultimately, self-defence measures by the injured party. This is why it is crucial for a lawyer to be present at all stages of cyber defence, so that they can properly analyze the facts, and translate them into immediate legal actions in the limited time given.

For example, what can we do if another State hacks into a critical military airbase causing fuel leaks which might later set off fires and explosions? What are the scale and effects of this attack, and what are our options, legally? Are we allowed to use active defence measures beyond our own networks? Can we take countermeasures under international law against that State, in order to end their unlawful act? Or, can we even use force in order to prevent the damage from materializing? Could it even trigger an armed conflict and if so, would that impact the measures we can legally take? What if there is no certainty about the identity of the attackers?

The examples given above were among the many different scenarios that the Agency's legal advisors had to analyze during Locked Shields. Participants had to provide legal answers within a limited timeframe to add a sense of reality to the exercise. This time pressure emulated the requirements of military commanders and political decision-makers in the conduct of operations. The teams were also assessed on the clarity of their answers.



Cyber-attacks, attribution and the law

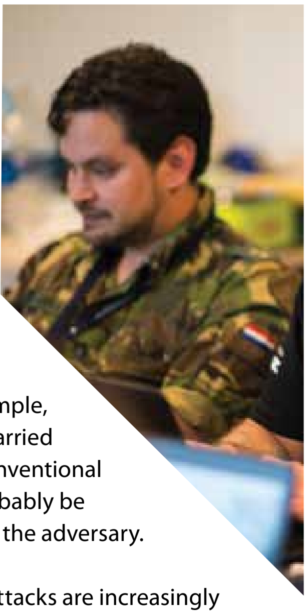
The law usually responds to new developments in society, but when these developments arise at the speed of a fibre-optic cable, lawmakers can have a hard time keeping up. While rules governing international operations already exist, many of them have not been interpreted for cyber operations yet. This is why lawyers need to run through contemporary cyber legal matters, and translate existing legal standards to the cyber domain.

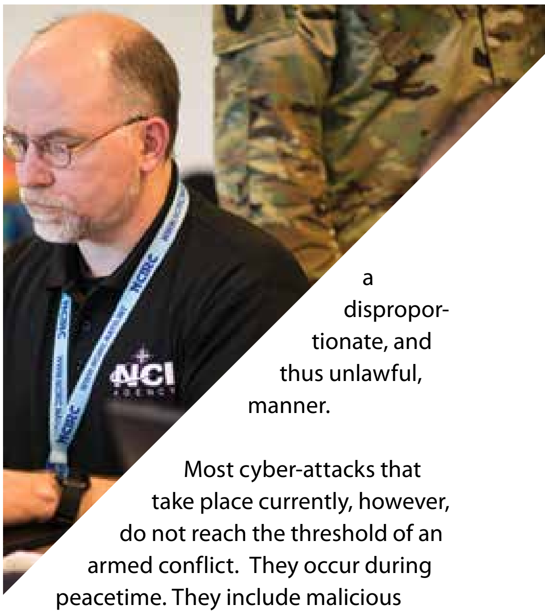
Recently-released books, such as the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, try to provide legal guidance, helping organizations interpret existing rules and legal norms in the cyber context. This guidance along with the ongoing analysis provided by lawyers during cyber operations, can ensure that a State's or an organization's (re-)actions to cyber-attacks have a legal basis. This in turn creates new customary rules based on state behavior.

It should be noted however that, even though these books provide scholarly guidance and practical tools to deal with cyberspace legal issues, many of the violations have not yet materialized. If they do, States may decide to respond very differently, and suggested legal actions or outcomes may not necessarily be followed by States.

Attribution can also be a source of difficulty during cyber operations. The victim of a cyber-attack has limited legal response options, which can be seriously hampered when the perpetrator's identity is not clear. Cyber security experts must be able to prove with reasonable certainty that a certain actor is behind malicious cyber operations for the victim State to take certain legal actions.

While the author of a conventional use of force can usually be identified with certainty very quickly, cyber-attacks usually involve techniques that will make it difficult to attribute the attack to a specific State or group. This can effectively prevent the victim State from obtaining the needed legal basis to respond under international law. Therefore, lawyers may need to look at the context of a cyber-attack to determine its nature. For example, cyber-attacks carried out during a conventional conflict will probably be associated with the adversary.





Also, as cyber-attacks are increasingly carried out by groups that only have a loose affiliation to the State where they are located, it is difficult to determine if that State is aware, involved with or even actively supporting the attacker.

If the State concerned refuses to provide assistance in stopping attacks from a group on their territory for example, then the injured party may at some point conclude that this State is either supporting the group or the attack or unable to prevent the attacks from happening. In that case, a legal advisor must determine whether the attack can still be resolved under the applicable law enforcement regime, what the options are under international law, and possibly if it may justify a military response.

Finally, the effects of a cyber-attack may be overestimated initially. What may appear as a major attack may only create minor damages in the long term. For example, a denial of service attack, like the one that occurred in Estonia in 2007, will render websites inaccessible for a certain period of time, but may not cause permanent damage or loss of data. And if the injured party were to retaliate with a military response too quickly, they would run the risk of reacting in a disproportionate, and thus unlawful, manner.

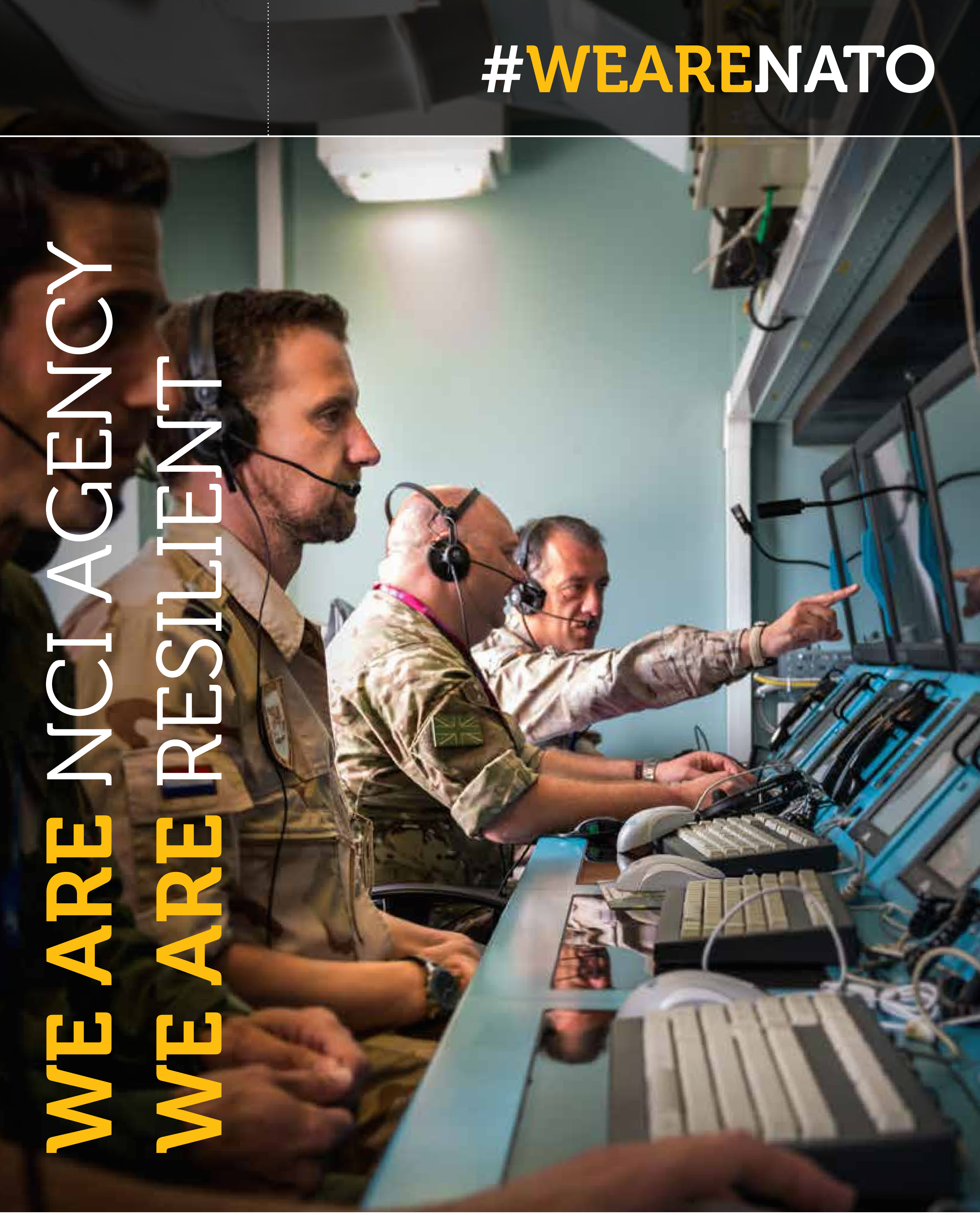
Most cyber-attacks that take place currently, however, do not reach the threshold of an armed conflict. They occur during peacetime. They include malicious activity such as breaking into military networks to steal classified information, espionage, website defacement and denial of service attacks.

Although these attacks may not be legally sufficient to trigger an armed conflict, they do not prevent the victim from taking steps to protect their network and infrastructure, for example by filtering or blocking network traffic coming from certain regions. Defensive measures can also contribute to gathering evidence against an attacker, and using it through international treaties for policing and judicial cooperation.

Conclusion

These examples highlight the need for legal staff to be constantly involved in cyber exercises, so as to simulate real-life decision-making processes, at all (political, operational, public relations and legal) levels. Exercises like Locked Shields help lay bare contemporary legal challenges and solutions and as such, provide deeper insight in the cyber domain.

By Nick Wobma, Legal Office



The NCI Agency connects NATO forces 24/7
so 29 Allies can work as one.
We provide resilient technology to the Alliance,
to save lives and safeguard peace.

NATO OTAN

NCI AGENCY

COMMUNICATIONS
SAVE LIVES
NCI
ONE NATO
WORKING TOGETHER
in
M-04
OPERATIONS
BEHIND THE SCENES
SUPPORT
ON THE GROUND
YouTube
NCI
AGENCY