Security Jam
Brainstorming global security

# The new global security landscape

## 10 RECOMMENDATIONS FROM THE 2012 SECURITY JAM


SDA SECURITY & DEFENCE AGENDA

IBM

European Union EXTERNAL ACTION

FONDATION pour la RECHERCHE STRATÉGIQUE

ATLANTIC COUNCIL

CHATHAM HOUSE Independent thinking on international affairs

CIDOB

Konrad Adenauer Stiftung

The Hague Centre for Strategic Studies

sipri

SWP 1962–2012

# Foreword

Our thanks and gratitude to all partners who contributed to the success of the 2012 Security Jam: first and foremost to the European External Action Service, the European Commission, NATO Allied Command Transformation, the U.S. Mission to NATO and the eight think-tank partners who moderated the debates: Atlantic Council of the United States, Chatham House, Centro de Estudios y Documentación Internacionales de Barcelona (CIDOB), Fondation pour la Recherche Stratégique, The Hague Centre for Strategic Studies, Konrad-Adenauer-Stiftung, Stockholm International Peace Research Institute (SIPRI), Stiftung Wissenschaft und Politik and the Jam coalition partners.

This year's extraordinary results wouldn't have been possible without the active help and encouragement of the following: **Admiral Jim Stavridis** (Supreme Allied Commander Europe, NATO), **General Stéphane Abrial** (Supreme Allied Commander Transformation, NATO), **Mike Ryan** (Deputy Director of Security, Cooperation and Office of Defense Cooperation (ODC) operations, U.S. European Command), **Leendert Van Bochoven** (NATO and European Defence Leader, IBM), **Maria Kokkonen** (Deputy Head of Division Strategic Communications, EEAS), **Vice Admiral Carol Pottenger** (Deputy Chief of Staff, Capability Development, NATO ACT), **Jamie Shea** (Deputy Assistant Secretary General for Emerging Security Challenges, NATO) and **Colonel Ross Thurlow** (Joint ISR Functional Specifications, NATO ACT).

There are no boundaries when it comes to sharing information and new ideas and it has been essential to involve all stakeholders and policy-makers. Building on the Jam's success in 2010, the 2012 Security Jam saw over **17,000 logins from 116 countries** with leading subject-matter experts and people from many walks of life taking advantage of our neutral online discussion platform.

We very much hope that NATO's and the EU's political leaders will take note of these recommendations and will further increase the use of new technologies to enlarge the involvement of citizens and stakeholders in the security policy debate. For its part the SDA will continue to offer a neutral platform for discussion and will experiment with new ways of sharing and exchanging ideas.

Giles Merritt
*Director*
*Security & Defence Agenda*

Geert Cami
*Co-Founder & Director*
*Security & Defence Agenda*

# Table of contents


| | | |
|---|---|---|
| **I.** | **Preface** | 2 |
| **II.** | **Introduction** | 3 |
| **III.** | **The 10 recommendations** | 4 |
| **IV.** | **Overarching issues** | 26 |
| | **1. Fostering global partnerships** | 27 |
| | **2. Developing the right tools for 21st century security** | 32 |
| | **3. Sustaining knowledge and expertise in new fields** | 43 |
| | **4. Future policy choices in a decade of austerity** | 48 |
| **V.** | **In conclusion** | 51 |
| **VI.** | **Live chats** | 52 |
| **VII.** | **Statistics** | 55 |
| **VIII.** | **VIP Jammers** | 59 |
| **IX.** | **Hosts and facilitators** | 61 |



**A Security & Defence Agenda report**
Author: Jonathan Dowdall
Publisher: Geert Cami
Project Managers: Pauline Massart and Andrea Ghianda
Design & layout: Mostra SA
Year of publication: 2012



**Disclaimer**
This report offers an independent analysis of the 2012 Security Jam for which only the author and the SDA can take full responsibility.
The views expressed in this report by individuals are personal opinions and not necessarily the views of the organisation they represent, nor of the Security & Defence Agenda, its members or partners.

The 10 recommendations were selected on the basis of their degree of innovation and pragmatism. They were not voted on.

# I. Preface

If the period between the 2010 and 2012 Security Jams is an example of the security landscape in the years to come, then defence and security organisations around the world will have an ample number of situations to deal with.

These will be further complicated by the broad ranging austerity measures that leave almost no defence organisation untouched. Government spending is clearly 'under the gun' and this will impact organisations' ability to deal with these security situations.

Just like companies cannot just cost cut their way to competitiveness and growth, defence organisations can not cost cut their way to more security and safety. It will require different and smarter ways to deal with both cost reductions and investments. The EU´s Pooling and Sharing initiative and NATO´s Smart Defence concept both aim to address these smarter approaches of dealing with security.

It is against this backdrop that the Security Jam brought a wide variety of stakeholders together from 116 countries to discuss security matters and to develop concrete ideas. This year's Security Jam has yet again proven to be an inclusive dialogue with actionable outcomes.

The new Jam platform leverages the approach that is common to the social media and helps to bring creative minds and organisations together in a network, facilitated by deep subject matter expertise. It is the power of these networks that can have a significant impact, but the real impact will ultimately depend on the leadership and courage to take the outcomes of the Jam and to turn them into actions for a better, safer, and more secure planet for all.

**Leendert van Bochoven**
IBM
NATO and European Defence Leader

# II. Introduction

It has been two years since the Security & Defence Agenda's 2010 Security Jam: the first effort of its kind to hold an open forum for discussing the world's most pressing security challenges. Yet the intervening two years have been as remarkable and troubling a period of international history as any before.

Europe's spiralling sovereign debt crisis and the slow, grinding path back to a budgetary balance in the U.S. has instigated a re-assessment of Western defence. Europe's impulse to slash defence spending has been tempered slightly by tentative attempts to cut the cost of military procurement – either through the EU's pooling and sharing, or NATO's Smart Defence.

In the U.S., meanwhile, the question of defence posture has been manifested in the 'Pacific pivot': the re-alignment of deployed forces to the Asia-Pacific rim at the expense of European commitments. Engagement with China has risen high on the diplomatic agenda of the decade ahead.

The major military commitments that have pre-occupied the U.S. have either been concluded (Iraq) or are rapidly approaching finalisation (Afghanistan). In 2011, the U.S. also announced to the world that the perpetrator of the largest terrorist atrocity in U.S. history, Osama Bin Laden, had been killed by a Special Forces intervention in Pakistan.

This milestone in the increasingly discredited concept of Global War on Terror (GWOT), coupled with new trends in drone-based targeted killings, marks a distinct phase in the global approach to international terrorism. At the same time, Somalia-based maritime piracy's continued expansion has highlighted the threat non-state actors can pose to global economic prosperity and security.

Meanwhile cyber-security, an issue discussed in the 2010 Jam as merely a 'non-traditional threat', has become a front-and-centre concern of international security. The large-scale intrusions of Western defence, government and industry networks, coupled with the revelation in 2011 of the world's most advanced cyber-weapon to date, Stuxnet, have made the topic of cyber-space central to the 2012 Jam. In this domain much uncertainty, and opportunity, is being identified, cast against the backdrop of an exponential and persistent escalation of cyber-attacks.

Perhaps most momentous of all on Europe's doorstep have been the sudden and largely unexpected democratic revolutions in the Arab world. These have destroyed old certainties in Tunisia and Egypt, the streets filled with youth and cautious optimism. In the case of Libya, NATO allies were called upon to deploy rapidly into a complex crisis situation, casting the recently under-used concept of responsibility to protect (R2P) principle back into stark relief on the global stage.

# III. The 10 recommendations

1 2 3 4 5 6 7 8 9 10


1 | NATO should formalize a maritime domain policy, to support the development of new common naval systems and platforms. 6

2 | NATO should create a NATO-China Council. 8

3 | The EU's Defence Industrial Policy should be updated, with a focus on pooling R&D, restricting sensitive exports and developing a new generation of military equipment. 10

4 | NATO should launch a programme dedicated to fostering a 'Smart Defence Mindset' amongst military personnel, national politicians and other stakeholders. 12

5 | Deployed nations in Afghanistan should establish a country-wide public education programme, to foster regional development post-2014. 14

6 | A cross-sectoral international 'coalition of the willing' of cyber-security professionals should coordinate confidence building measures for cyber global governance. 16

7 | 'White hat' hacker recruitment should be incorporated into public cyber-security policy. 18

8 | The EU should launch a career scheme for training crisis management professionals and create a pool of commonly funded crisis management equipment. 20

9 | Crisis management stakeholders should create an online community and knowledge hub for informing operational staff. 22

10 | Western allies should establish a more comprehensive authorization process and doctrine for planning and launching 'responsibility to protect'-based military interventions. 24

1 2 3 4 5 6 7 8 9 10

**NATO should formalize a maritime domain policy, to support the development of new common naval systems and platforms.**

From maritime piracy against international shipping to arctic security and the new realities of rising naval powers in the Far East, Jammers focused on maritime technology as a key area in need for coordination. NATO should formalize a maritime domain policy that anticipates ships operating beyond the Euro-Atlantic area more regularly, to map out member state programmes and to push for new common platforms.

**Magnus Nordenman**, Deputy Director of the Program on International Security at the Atlantic Council of the United States, stated that 'maritime operations are a real future "business opportunity" for NATO, and I think it is already relatively well equipped, trained and exercised to take it on'.

Whilst agreeing that a new generation of naval platforms would be needed to sustainably assert such a stance in maritime spaces beyond the Euro-Atlantic area, Nordenman added that 'the Alliance has enough hulls and manning to take this on' immediately.

**Michael Hannan**, Commander in the U.S. Navy and Federal Executive Fellow at the Atlantic Council of the United States, agreed that a more formal maritime policy by the Alliance could help support the U.S. navy as it copes with its own over-stretched budget. 'Transitioning from a "U.S. does it all" concept to shared responsibilities and supporting European nations to take the lead on efforts in which they are already engaged is a smart move – both for the U.S. and to bolster European involvement in global security'.

Many Jammers felt that NATO should also be supporting the development of more flexible, small-scale naval assets, augmented by un-manned systems and the latest maritime surveillance software. **Dennis Prange**, Defence Analyst, said such a focus should 'enforce a cultural change in the Navies, away from the increasingly expensive big platforms towards more decentralized solutions'.

'While I do not see that change of mind coming anytime soon for the U.S. Navy, it might soon be a financially imposed reality for the Europeans', Prange added. This mirrors calls from many Jammers that the current financial crisis offers Alliance members a chance to prioritise their maritime investments.

1 2 3 4 5 6 7 8 9 10

*Chinese representatives taking part in official side events of NATO summits would be a clear signal for NATO's understanding of the current landscape of relevant global security actors.*
**Giles Merritt, Security & Defence Agenda**

## NATO should create a NATO-China Council.

In light of China's increasing global influence and clear military build-up, NATO should establish a NATO-China Council (NCC) to mirror the alliance's engagement within the NATO-Russia Council.

Such a platform, Jammers argued, would help establish stronger diplomatic and personal connections with Chinese counterparts both within the Alliance and at national level. The NCC would also offer a formalized platform for confidence building and mutual understanding.

As **Giles Merritt**, Director of the Security & Defence Agenda, explained, 'a dialogue platform with Beijing might represent an important strategic move from a global governance perspective... This would show China that it is taken seriously by the transatlantic community, and would give the West a better understanding of intentions behind China's military build-up'.

Suggested areas of cooperation include the stabilization of Afghanistan post-2014, maritime piracy, energy security and nuclear non-proliferation. **Emma Scott**, an Irish International Relations student, also noted that the Shanghai Cooperation Organisation (SCO) – the regional security organisation of which China and many Central Asian nations are members – operates a number of counter-terrorist programmes which could foster collaboration.

'The SCO has already established the Regional Anti-Terrorist Structure (RATS) in Tashkent... NATO would definitely have a lot to contribute to improve the effectiveness of the RATS', she opined.

The potential for the SCO to sit as an observing or even a contributing member in the NCC was encouraged by Jammers. **Agnieszka Nimark**, Associate Researcher at CIDOB felt that a potential NCC should provide a point of contact between NATO and the SCO. She argued that due to the asymmetry of membership (28 vs. China), the SCO would act as an influence multiplier on the Chinese side. Thus, 'China [is] more likely to establish a dialogue/security forum with NATO when invited to the table as the SCO', Nimark suggested.

However, Jammers also acknowledged the potential limitations of an NCC. Some noted Chinese reticence about the alliance's core values. Indeed, there was concern that engaging with the SCO – whose member governments are largely authoritarian in character – might be diplomatically difficult. Others questioned whether the majority of NATO members hold too limited a regional military influence in the South China Sea and other areas of strategic Chinese interest to offer real value.

In countering these concerns, Jammers pointed out that due to the range of complex international issues – particularly economic – in which China has a voice, an NCC would offer a specialist forum to focus on defence and security. As **Juan Garrigues**, Research Fellow at CIDOB noted, the EU has often found its security affairs relationship with China muddied by other political issues.

For instance, 'the EU has cooperated with China in security challenges such as securing maritime routes, but divergences on other issues such as trade relations or Syria has generally limited cooperation'. An NCC, in being solely security focused, might avoid this conflict.

As Merritt explained, 'NATO dialoguing with China would give Beijing a clear idea of the values and intentions of the transatlantic community in total, [but] would at the same time not prevent parallel talks between the U.S. and China or the EU and China'.

An NCC would thus offer clear security policy added value for both China and Alliance members.

1 2 3 4 5 6 7 8 9 10

*Sharing is of key importance, also requiring Member States' support to industry through continued definition of European key industrial capabilities.*
**Claude-France Arnould, European Defence Agency**

## The EU's Defence Industrial Policy should be updated, with a focus on pooling R&D, restricting sensitive exports and developing a new generation of military equipment.

Jammers explored a wide range of military equipment currently missing, or operated in insufficient numbers, amongst European militaries, creating a strategic reliance on the U.S. and ham-stringing European security goals.

As **Claude-France Arnould**, Executive Director of the European Defence Agency (EDA) explained, the EU's Pooling & Sharing (P&S) programme for military equipment, in coordination with NATO's Smart Defence initiatives, is one solution to this problem. However, she added that 'longer term industrial aspects require attention to avoid increasing future European external dependency'.

To bolster these industrial efforts, Jammers argued that the European Commission's 2007 Defence Industrial Policy, and its prime achievement thus far, the Defence Directives on defence procurement and intra-community transfer, should be updated to more directly support a new generation of European military technology.

Jammers want the policy to focus more strongly on investment goals in military R&D, and the possibility of pooling and sharing research in multi-lateral technology projects. **Marius-Eugen Opran**, a delegate of the European Economic and Social Committee Consultative Commission for Industrial Changes (EESC – CCMI), argued that the EDA should have a more direct role in coordinating R&D collaboration.

He said that if Europe is to successfully produce a new generation of 'made in Europe' military equipment, 'the Commission and member states' main task will be to increase exponentially the EDA R&D allocated budget', whilst 'working more closely together through the EDA'.

Better coordination is also required if European technology projects are to be developed, procured and deployed in line with rapid advances in technology. Jammers cited projects such as the Eurofighter and A400M transport aircraft, that have come in vastly over-budget and almost a decade behind schedule, as a sign of these problems.

**Leendert van Bochoven**, NATO and European Defence leader at IBM explained that the military development 'cycle needs to speed up as the overall pace of the technology cycles increases. We see a constant commoditization of the technology layers, and will have to outpace that in order to stay relevant'.

A focus on the small and medium enterprises that underpin the defence sector was also recommended by Jammers, who claimed such firms are often the source of rapid technological innovation.

Others highlighted the necessity of keeping certain highly sensitive technology within Europe. An anonymous jammer said that 'we are currently committing a collective suicide in transferring high-end knowledge to emerging powers (aircraft, submarine, missiles)... we have to strengthen agreements on technology transfers from our nations to others'. They and others thus advocated an EU restriction on certain forms of technology exports, in a similar fashion to the U.S. 'ITAR' arms transfer regime.

The new policy should also be directed towards supporting direct EU funding for research into 'dual-use' areas such as maritime surveillance, unmanned systems and logistics support. They commented that dual-use technology can 'entail huge benefits for civilian industry and employment'.

Opran agreed, arguing that 'the new 8th Framework Programme (also known as "Horizon 2020") European Security Research Programme must co-finance military technology developments which might lead to dual-use applications'.

1 2 3 4 5 6 7 8 9 10

*In my interactions with Nations, I have sensed a strong desire for the emergence of such a mindset.*
**Gen. Stéphane Abrial, NATO Supreme Allied Command Transformation**

**NATO should launch a programme dedicated to fostering a 'Smart Defence Mindset' amongst military personnel, national politicians and other stakeholders.**

Jammers agreed that Smart Defence is about more than simply saving money. It requires national politicians and military staff to think in a new, collaborative mindset when it comes to procuring and operating their military equipment. As NATO Supreme Allied Commander Transformation (SACT), **General Stéphane Abrial** told Jammers, 'Smart Defence is not about doing more with less. It is about doing better with the resources we have, in order to fulfil the Alliance's level of ambition'.

This is what the SACT calls the 'Smart Defence Mindset', and Jammers asserted that NATO should focus on formally supporting this way of thinking amongst Alliance members.

Inculcating this mindset requires a 'whole of government' debate about the potential benefits, but also costs, of committing to Smart Defence projects. An anonymous jammer argued that officials at the 2012 NATO Chicago Summit 'need to go back to their governments and make sure the ideas are accepted within all departments of the government'. He added that 'we have to acknowledge it is not only within Departments of Defence these ideas have to be adapted and carried forward. They certainly also have to be adapted within ministries of economics, industrialisation, departments of justice etc'. This focus on all relevant stakeholders will help break down barriers in the proposed programme.

General Abrial also noted the industrial concerns of the Smart Defence Mindset. 'National (or multinational) industries are often part of a nation's core interests. This needs to be taken into account', he said.

**Leo Michel**, Distinguished Research Fellow at the Institute for National Strategic Studies, National Defense University, agreed that 'there's potential for tension on many fronts, arising from different state-industry relations depending on the Ally/Partner involved [and] direct or indirect competition for military sales both within and outside the Alliance'.

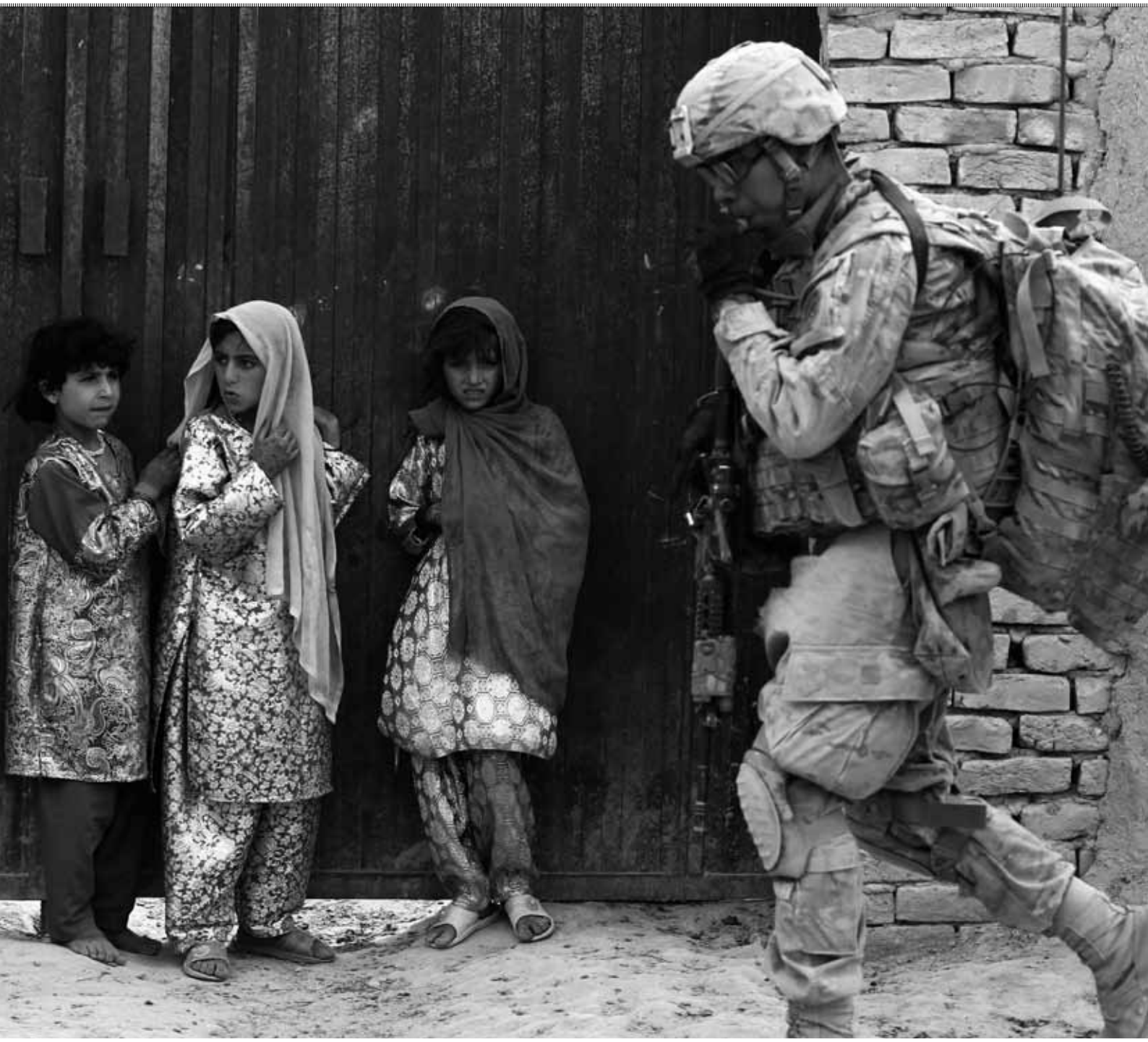
To address this, Jammers suggested that the potential benefits of Smart Defence for industry need to be more strongly communicated. As an anonymous jammer explained, 'a cultural change is required with all stakeholders... the smart way is a close interaction from the earliest steps of capability development. This creates an informed customer and an informed provider'.

Summarised as 'moving from a "hands-off" to a "handshake" approach' with industry, the anonymous jammer argued that a greater appreciation of the industrial advantages in the Smart Defence Mindset could ease further cooperation between industry.

Given Smart Defence's call for cross-border equipment sharing, it will also test levels of bilateral trust between nations. An anonymous jammer advocated advancing pragmatic cross-border relationships for building such trust. 'Simply developing a habit of acquiring and managing our collective capabilities, and making sure that we have the right structures and processes in place to do so, will also build trust', he pointed out.

Whilst primarily a discussion that needs to be had at national level, Jammers also suggested that this outreach programme could focus on the resources of the NATO Parliamentary Assembly – the alliance's body for engaging with national parliaments. Given the potential ramifications for national defence policy of sharing equipment, a key sovereignty concern, Smart Defence 'must be submitted for due democratic scrutiny', one Jammer opined. This should include a wide consultation with stakeholders from the public and private sectors.

1 2 3 4 5 6 7 8 9 10



> *A more informed citizenry is the first step towards peace, irrespective of culture or geography.*
> **Ijaz Khan, University of Peshawar, Khyber Pakhtunkhwa**

**Deployed nations in Afghanistan should establish a country-wide public education programme, to foster regional development post-2014.**

With international military engagement in Afghanistan facing a rapid reduction in 2014, deployed nations should focus on creating a viable public education programme, capable of being sustained in the absence of direct Western support. The ideal model for this would be an 'e-learning' system – supported by internet infrastructures capable of being operated in remote regions – to facilitate literacy and health education programmes.

Jammers, whilst acknowledging the current paucity of ICT back-bone in Afghanistan, felt that public education was an urgent priority in the wake of NATO's formal hand-over to Afghan forces. As an anonymous jammer explained, 'education is a multi-generational fix requiring a significant, long-term commitment from students, educators, and institutions'.

By providing the ICT tools to support that commitment, Alliance members can build on 'the renewed emphasis on literacy training, including mandated classes for Afghan National Security Forces and the Radio-delivered Literacy Programs for children', they added.

Jammers also argued that by simply providing the ICT infrastructure needed for Afghans to connect to regional civil society and educational programmes, the programme could be rendered 'a-political', and thus more widely acceptable. **Michael Ryan**, Deputy Director, Policy, Strategy, Partnership and Capabilities at the U.S. European Command, agreed that an effort to plug Afghanistan into regional networks is important. 'Afghanistan is isolated. Isolation is why it is the way it is. The region needs to be connected economically and intellectually to the global consciousness'.

Other Jammers questioned whether Afghan citizens would welcome a greater emphasis on education, especially given the hostility towards female and non-religious education shown by many groups. However, **Ijaz Khan**, Professor of International Relations at the University of Peshawar, Khyber Pakhtunkhwa, Pakistan, argued that the universal desire for peace in the country would overcome these nuances. 'A more informed citizenry is the first step towards peace, irrespective of culture or geography', he said.

Others, felt that common goods such as ICT support and education programmes will help impact what an anonymous jammer called the 'human environment' in the Afghan conflict. This is that 'the most important effects achieved are not the kinetic ones, but the social and psychological: what people perceive and how they respond to it... Technology and future capabilities should support these aspects as eagerly as it supports the kinetic ones'.

An additional advantage of this approach according to Jammers is that, in light of the billions spent by military forces thus far in Afghanistan, even a large-scale ICT investment would likely be a cheap policy option in relative terms.

As Ryan affirmed, 'the spin-off benefits in this day and age of building "digital natives" in an unconnected place like Afghanistan, in addition to the primary benefit of creating "unintentional functional literacy" (i.e. Learning to read through ICT training), seem to far outweigh the cost'.

1 2 3 4 5 6 7 8 9 10

*Work should be going on in international fora to come up with codes of conduct and responsibility in cyberspace.*
**Vytautas Butrimas, Lithuanian Ministry of National Defence**

## A cross-sectoral international 'coalition of the willing' of cyber-security professionals should coordinate confidence building measures for cyber global governance.

Jammers were generally united in calling for a treaty based, internationally recognized 'cyber-space convention' – be it through an arms-control model or a normative, 'rules of the road' approach.

However, as one Chatham House participant observed, 'setting up such a mechanism for international collaboration is a long-term process'. Given this, significant confidence building will be need between nations before they can collaboratively handle emerging cyber-threats. In the interim, cyber-threats will continue to proliferate.

Jammers thus advocated that key cyber-security stakeholders and experts should form a 'coalition of the willing' set of working groups to help disseminate new ideas, assess emerging threats and generally assist governments and national agencies whilst a more formal global mechanism is established.

**Vytautas Butrimas**, Chief Adviser for Cyber Security at the Lithuanian Ministry of National Defence, said that such groups should mirror the actions undertaken by 'a voluntary group of experts and institutions that banded together to contain the spread of the notorious Conficker worm'. (Conficker was a highly intrusive and covert exploit against Microsoft operating systems, first detected in 2008).

He explained that 'nobody told them to work together, they just decided out of their understanding of the Internet and the threat of this worm to cause havoc to our online world that action was needed'.

However, some Jammers argued that such an effort would suffer from the 'chicken and egg' syndrome inherent to current cyber-governance efforts. They claimed that without common understandings of cyber-security norms, experts cannot coordinate; whilst without coordination, norms cannot be agreed upon.

**Jamie Shea**, Deputy Assistant Secretary General for Emerging Security Challenges at NATO, disagreed that this would be an obstacle, arguing that a universal feeling of 'victimhood' to hacker intrusion will bypass petty disagreements.

After an attack 'you are instantly the victim, as someone is interfering with your legal right to privacy and the enjoyment of your freedom to go about your business normally'. Given this, 'I believe that we should not waste too much time trying to distinguish between cyber-attacks', and instead get down to the business of preventing them, Shea argued.

Whilst similar in many ways to existing industry-based information sharing groups on cyber threats, the key distinction of this model would be an emphasis on public discussion, to help eventually hone down an internationally agreed cyber-space treaty.

As Butrimas explained, 'this information could act as a form of 'soft public pressure' on nations to respond to reports of cyber attacks originating or transiting through their "cyber jurisdictions" '.

Such confidence building, in parallel to national diplomatic initiatives, could lay the foundations for a safer and more secure cyber domain.

1 2 3 4 5 6 7 8 9 10

*[We must] make it more attractive for hackers to become a part of and defend the system.*
**Norica Nicolai, European Parliament**

## 'White Hat' hacker recruitment should be incorporated to public cyber-security policy.

The best expertise in the cyber domain can often be found amongst the hacker community – private citizens who have actively engaged in exploring, and sometimes breaching, the boundaries and capabilities of the online world.

To overcome the scarcity of cyber-security talent in the European public sector, Jammers recommend that public agencies in the EU and member states should replicate the private sector practice of hiring hackers under so-called 'White Hat' schemes.

White Hat programmes consist of talented individuals being invited to deliberately intrude and test the security of a company's systems. As **Igor Garcia-Tapia**, Project Manager at the Security & Defence Agenda explained, 'many organisations in the private sector have set up white hat programmes whereby hackers are paid for any weaknesses and gaps they find. In this sense the private sector is well ahead of the public sector'.

**Benoit Baufays**, a Belgian IT Student, agreed that private sector practices are working, and should be imitated to secure public networks, infrastructure and data. 'I think that the best way to approach and recruit people with real skills (and not only young scholars) is to imitate companies such as Google, Amazon and Facebook', he said.

Romanian MEP and Vice Chair of the European Parliament Subcommittee on Security and Defence **Norica Nicolai** agreed, stating that public agencies should try to 'make it more attractive for [hackers] to become a part of and defend the system', instead of trying to hack it.

Other Jammers added that such schemes could help bring potentially dangerous actors into the security community. As **Pauline Massart**, SDA Senior Manager explained, Europe's high rate of unemployment amongst young people is leaving a large number of 'idle hands' in cyber-space, which could prove problematic in future. 'Could the worsening financial crisis push people who have the skills towards damaging intent?' such as cyber-crime or sabotage, she asked.

However, questions remain unanswered about the potential legal, security and technical difficulties of allowing government agencies to hire private individuals in this manner. Some Jammers were uncertain if sufficient security vetting of applicants could be assured. Others added that the financial incentives offered by the private sector for White Hats may be beyond the means of the public sector.

Despite these concerns, **David Clemente**, Lead Cyber Security Researcher at Chatham House, pointed out that there are the beginnings of open-source recruitment for cyber-security already in Europe, in the UK. 'The search to unearth talent takes many forms, and one of the most successful UK examples is the Cyber Security Challenge', an online test where coding puzzles are used to track down potential recruits for specialist agencies such as GCHQ – Britain's intelligence centre.

Indeed, despite these potential stumbling blocks, high-level Jammers agreed that harnessing cyber-talent was a pre-requisite to better cyber-security. As NATO SACT General Stéphane Abrial told Jammers, 'Our people are our best line of defence'.

Jammers thus argued that officials must not allow prejudices or fears about hackers to blind them to the advantages of such a scheme.

1 2 3 4 5 6 7 8 9 10

*We rely on our network of EU delegations across the world and on our own scoping missions to crisis spots. There is nothing like being on the ground if you want to understand the real issues at stake.*
**Agostino Miozzo, European External Action Service**

## The EU should launch a career scheme for training crisis management professionals and create a pool of commonly funded crisis management equipment.

The EU lacks a formal career path for crisis management professionals, and Jammers agreed this creates the risk of corporate knowledge and field expertise being lost. EU member states also often lack the inventories of specialist equipment for crisis situations – from aircraft to field hospitals and search and rescue – required for rapid deployment in a crisis scenario.

It is time to concentrate on making sure the generation of field-experienced crisis management professionals the EU has fostered in the past decade are secured within the European External Action Service system. The EU should also commonly fund the purchase and storage of the equipment such staff need in a crisis situation.

**Justin Davies**, Managing Director of C2M Solutions in Belgium, lamented the lack of vocational training in civilian crisis management. 'There is no such thing as a "crisis response professional"... there's no college you can go to, degree you can study or career path that you can follow'. As such the EEAS should 'put in place some career planning so that the new, young EU crisis desk officers of today can be experienced EU crisis response leaders in 30 years time'.

This new career path should include ample time abroad, space for specialist training and incentives to draw talent with relevant national, private sector or NGO experience to work in the EEAS. 'I don't see this happening at the moment', Davies said.

Some Jammers also complained that existing departments such as DG ECHO (the European Commission's crisis management and humanitarian assistance Directorate General) are not necessarily willing to share experienced staff when needed. Davies explained that 'the EU is notoriously mean at allocating new posts in HQ when new missions are established... which is one of the reasons why EU lessons-learned is in such a pitiful state'.

This career scheme would ideally complement ongoing EEAS efforts to streamline its crisis management functions. As **Agostino Miozzo**, European External Action Service Managing Director for Crisis Response and Operational Coordination, explained, the EEAS is currently in the process of bringing together, through the EU Crisis Platform, 'various crisis response/management structures as well as relevant geographical and horizontal EEAS departments, and the relevant services of the European Commission and the General Secretariat of the Council'. This platform could be the hub from which staff embarking on this new career structure would operate.

Jammers also argued that as crisis management equipment is expensive to both purchase and operate, an EU funding scheme for such assets could be cost effective. **Jonathan Dowdall**, Brussels-based journalist and policy analyst, explained that such a system would have a threefold advantage over current, member state-based voluntary systems:

'1. EU owned equipment would always be available, and could not be withdrawn by member states due to domestic concerns or double-booking. 2. EU owned equipment could be purchased at a good economy of scale, and stored/maintained in pooled facilities which would be cheaper than individual member state storage. 3. EU owned equipment would not be subject to the vagaries of member state budget negotiations or the strength of market forces: the Commission would simply invest in those assets needed for certain types of crisis'.

**Ian Anthony**, Research Coordinator at SIPRI and Director of the Programme on Arms Control and Non-proliferation, agreed that a carefully chosen list of equipment could be ideal for such a scheme. 'From past experience, we know the types of capability that tend to be in short supply or difficult to mobilize at short notice'.

Other Jammers noted that the recent addition to the mandate of Frontex, the EU border agency, allowing it to own and operate its own equipment, could become a precedent. A member of a German university **Cathleen Berger** added that, 'especially since such developments within EU agencies often spill over into other agencies once the model is established... this might lead to EU owned equipment in this area as well'.

1 2 3 4 5 6 7 8 9 10

> *It is really a central problem of contemporary crisis management: the lack of case-specific and country-specific information.*
> **Marco Overhaus, German Institute for International and Security Affairs (SWP)**

## Crisis management stakeholders should create an online community and knowledge hub for informing operational staff.

An insufficient appreciation of local conditions in states undergoing a crisis, which must exist to formulate a culturally nuanced mission plan, is a serious information deficit in contemporary crisis management. Jammers suggested that to overcome this, an online environment dedicated to pooling the collective expertise of stakeholders from across sectors and borders should be set up.

Jammers thought that such an environment would allow experts with field experience in the crisis-hit nation or conflict zone to liaise directly with incoming staff, share ideas and observations with national officials and give a free source of information to cash-strapped civil society groups or NGOs.

As **Marco Overhaus**, Senior researcher on European Security and Defence Policy at the German Institute for International and Security Affairs (SWP) explained, 'it is really a central problem of contemporary crisis management: the lack of case-specific and country-specific information'.

He joined other Jammers in criticising the amount of contextual information available to deployed military and civilian personnel in theatre. 'In Afghanistan, one of the many problems seems to be right from the beginning that the "coalition of the willing" under U.S.-leadership and subsequently NATO did not have sufficient knowledge about politics, culture, tribal dynamics etc. in the country', Overhaus said. 'The same holds true for Libya'.

To overcome this, **Michael Ryan**, Deputy Director of Security, Defense Cooperation at the U.S. European Command (U.S.EUCOM), opined that 'such a forum could be a physical location where actors assign experts to work together to come up with the best methods of collaboration, the best planning tools, the best communication methods for coordination on the ground, the best ideas for how to deal with various scenarios, in other words, a place where real people work together on real problems'.

Ryan referenced the work of **Leo Michel**, Distinguished Research Fellow at the Institute for National Strategic Studies, who has also forwarded a similar concept called the International Community Planning Forum (ICPF). Michel advocates the step-by-step build up of such a platform based on working groups and regular meetings.

'One could imagine, for example, starting with a series of focused workshops hosted (or co-hosted) by nations such as Finland, Sweden, Norway and Denmark – all of which have excellent experience in the field', Michel explained.

Some Jammers did express concern that the mixture of stakeholders sharing information in such a forum could prove difficult, particularly between military actors and NGOs. **Chad Briggs**, Minerva Defense Fellow and Chair of Energy and Environmental Security at the Maxwell AFB Air University, cautioned that 'this can be difficult, especially in cases where the NGOs have to appear impartial' .

He added that 'another big issue is secrecy, since as in all security organisations, information flows tend to go one way, it's difficult to establish information sharing... and NGOs are less likely to share except in unclassified space'.

Yet despite these concerns, Jammers avowed that the potential of online information sharing should be seized. Ryan maintained that, with such information, 'unlike what happened in Afghanistan, we'd have a chance of doing the essential things right, and doing them right early enough to make a difference'.

1 2 3 4 5 6 7 8 9 **10**

**Western allies should establish a more comprehensive authorization process and doctrine for planning and launching 'responsibility to protect'-based military interventions.**

Many Jammers noted that during the NATO-led Operation Unified Protector over Libya, the application of the responsibility to protect (R2P) principle of humanitarian intervention may not have adequately appreciated the political, economic or social 'end game' that such an operation would entail.

A more comprehensive authorisation process should be reviewed and established for future Western-led R2P operations, based around planning for a clear political end-state strategy, post-conflict management scheme and strong commitment to avoiding civilian casualties.

As an NGO Jammer noted, whilst the intervention was broadly successful, the current state of Libya calls some of the R2P principles of the NATO intervention into question. 'It seems that with around 300 active militias the serious possibility of the division of the country between east and west, and the National Transitional Council having only extremely limited political legitimacy... more should have been done to think through likely consequences of bringing down the regime', they opined.

An academic Jammer agreed that whilst the military conduct of Allied forces over Libya was rightly focused on the specific objectives of eliminating the threat to civilian areas, this may have neglected the conditions needed to establish a stable country post-intervention. 'The "race of Tripoli" priority, whilst noble, may not have constituted a comprehensive strategy', they said. 'Could more have been done in the planning phase to avoid some of today's problems?'

One idea raised to meet these challenges came from **Joris van Esch**, Strategic Analyst at the Hague Institute for Strategic Studies, who drew attention to a Brazilian doctrinal initiative from 2011 known as 'Responsibility while protecting'. (RWP)

RWP, van Esch explained, suggests a more precise set of justifying criteria for utilising UN sanctioned force. This includes 'the need to exhaust all peaceful means before considering the use of force' in a more thorough way, whilst also calling for 'the monitoring of UNSC sanctioned force' to assure it does not unduly over-step the forces levels necessary.

The focus should be on multi-national training for intervening under the R2P banner, including tactical doctrines designed to mitigate the risks of complex operations with a high potential for accidental civilian casualties. Other Jammers added that a more subtle and contextually specific use of R2P, that takes into account the potential 'cascade effects' of intervention, will be the only way to revitalise this policy option in the coming years.

# IV. Overarching issues


Jammers focused on a wide range of topics and themes. Yet across borders, age groups, professions and points of view, some common ideas and thoughts nonetheless emerged about the state of contemporary global security.

These overarching areas of discussion, and recommendations on how to proceed, are summarised below.

1. **Fostering global partnerships**
2. **Developing the right tools for 21st century security**
3. **Sustaining knowledge and expertise in new fields**
4. **Future policy choices in a decade of austerity**

# 1. Fostering global partnerships

## All eyes on China

China quickly emerged in the 2012 Security Jam as the most intensely debated country. As **Agnieszka Nimark**, Associate Researcher at the Spanish think-tank CIDOB noted, this is predominantly due to the 'increasing perception of China as America's emerging rival in global preeminence'.

Whilst this focus on competition was a common theme, Jammers generally seemed more interested in 'understanding' China than deciding how to combat its growing global influence. The consensus was that, in light of the U.S. 'Pacific Pivot', a clear increase in Chinese military power and the relative decline of European global influence, Beijing will soon be an important partner in a host of global security issues.

Many were quick to note encouraging levels of cooperation between China and other international actors. **Riley Barnes**, Assistant Director of the International Security Program at the Atlantic Council of the United States, noted trending Jam discussions on maritime security, counter-terrorism and energy security as ongoing examples of common ground for dialogue with China. Jammers also identified nuclear non-proliferation and disarmament policy as a top priority, where China's key relationship with the recalcitrant North Korea could prove vital.

However, opinions were more divided over complex problems such as global cyber-security, where China was universally identified as a 'problem actor'. **Jason Healey**, Head of the Cyber Statecraft Initiative at the Atlantic Council of the United States, noted that alongside Russia, China remains one of the only actors who possesses the potential capability 'to really cause long-term, massive disruption – to take down critical infrastructure and then keep it down even in the face of the defence's best efforts'.

Though few Jammers felt China currently has the intention to go ahead with such a large-scale action, the potential capability clearly moves China into a distinct category in terms of cyber-defence and security policy.

Another area seized upon by Jammers was the stabilization of Afghanistan after NATO's predicted 2014 end of combat operations. Noting that China is becoming a major economic investor in Afghanistan **Jaap de Hoop Scheffer**, former NATO Secretary General and SDA Co-President, pointed out that 'the minimum one should try (success far from guaranteed) is a scenario where Afghanistan's "neutrality" is respected by the many nations having an interest in its future'. For this, he noted that China is increasingly relevant, and should be encouraged to view Afghan stability as a common good for the region.

'NATO-China' was
the highest trending subject
in the Strategic Partnerships forum.

Underlining all of these suggestions was an appreciation that engaging China will require a degree of adaptation by Europe and the U.S.. **Silvia Sartori**, a China based international development professional, pointed out that the Chinese culture and mindset are 'distinctively pragmatic'. In this context, Europe in particular may need to change the way it operates when talking with Beijing.

'China wants to engage more with Europe, but is often put off and confused by the complexity and bureaucracy of Europe itself', an anonymous jammer warned. 'The European modus operandi sometime does not seem pragmatic at all to them'. This warning was echoed throughout the Jam – the EU will need to adjust and hone its diplomatic methods if it wishes to deal with Beijing more successfully.

**Daniel Fiott**, a Research Fellow at the Madariaga College of Europe Foundation, also observed that 'China responds to security threats on an ad hoc basis', and is often more concerned with 'interests' than 'frameworks'. Given this, though creating a more permanent forum for security discussions, such as a NATO-China Council (See Jam Rec. 2), could be helpful, U.S. and European partners will also need to accept that they may have to approach Beijing on a more ad hoc basis than they are perhaps used to.

Jammers were nonetheless certain that China also has an interest in fostering these new global partnerships. 'China often wants to be a stronger participant in the international arena,' Sartori explained, 'where it still often feels "marginalized" '.

Decreasing this sense of marginalization, be it through ad hoc arrangements, the EU or NATO, is clearly a priority.

## Towards a global 'cyber-convention'?

Another high-trending Jam topic revolved around cyber-security, and specifically, the issues of global governance and mutual agreement that would be required to formulate a binding cyber-space security convention; akin to the Geneva Convention on conduct in war.

For some Jammers, the inability of international actors to agree on any common 'rules of the road' in cyber-space were due to the faulty premises being used to understand this domain. A heated debate about cyber-space as a 'global commons' highlighted this, with Jammers unsure if a domain owned and operated by Internet Service Providers (ISPs) can truly be called 'common'.

Even the most basic premises of deterrence and defence in cyber-space were sometimes questioned. Romanian MEP and Vice Chair of the European Parliament Sub-committee on Security and Defence **Norica Nicolai** provocatively suggested that there was no logical reason to fear large-scale cyber-attacks at all. 'Attacking servers in the U.S. might kill revenues in Asia, for example. It might very well be a case of mutually assured destruction'. Under such conditions, why wouldn't states want to seek a common agreement in the model of nuclear non-proliferation?

Indeed, Jammers generally felt that concepts such as 'cyber-war' have been over-hyped, and do not reflect the current threat environment or growing international willingness to cooperate. As **Igor Garcia-Tapia**, Project Manager at the SDA noted, there is a clear divide between state actors capable of causing damage and terrorist or non-state elements who may desire widespread destruction.

'With regards to "cyber Pearl Harbours" and "cyber 9/11"... those with the capability lack the intent and those with the intent lack the capability', he claimed.

Op-ed

# European External Action Service

Security challenges have become increasingly complex, unpredictable and cross-border. They are no longer an issue for governments alone. Hence the added value of involving a wider public of security experts and interested people from different parts of the world in security debates: the Security Jam provides such a platform. This year's edition of the Jam again covered a very broad range of issues, as demonstrated by the ten selected recommendations.

From the European External Action Service perspective, I would like to pick up a few points:

- the need for comprehensiveness: a crisis needs to be addressed in a comprehensive manner, using all available instruments in a coherent manner, and working closely with partners. The EU can use a wide variety of instruments and is uniquely placed to continue developing such an approach.

- the initiatives on Pooling and Sharing within the EU and Smart Defence within NATO complement instead of duplicate one another; this is a good example of partnership which is being highlighted in the run up to the NATO Chicago Summit.

- the international discussion on how best to address cyber challenges has gained momentum; international cooperation and the application of existing legal frameworks such as the Council of Europe Convention for Cybercrime, the Human Rights law and the International Humanitarian law are the most promising way ahead; in the EU we are considering the development of a broad based approach, involving all relevant aspects (human rights, security, economic and industrial) as a building block of a global framework.

**Maciej Popowski**,
Deputy Secretary General
for Inter-institutional Affairs,
European External Action
Service (EEAS)

EEAS

**Op-ed**

# NATO Allied Command Transformation (ACT)

One of ACT's major objectives is the transformation of NATO. This means leading, facilitating and advocating change and continuous improvement of Alliance capabilities in order to maintain and enhance the relevance and effectiveness of the Alliance; future security is our business. However, to achieve this we need to understand and account for the views and thoughts of all communities with a stake in security. In other words we need to take a comprehensive approach to solution finding. Therefore, ACT viewed the Security Jam as a forum to demonstrate our desire to participate in a wide debate on security issues in order to take advantage of any interesting or innovative ideas that may arise during the event. We also saw the Jam as an innovative approach in and of itself, one that provides a unique opportunity for our staff to interact with individuals from many different backgrounds with differing views. As we continue to develop, improve and embrace activities like the Security Jam, the resulting increased intellectual reach and connectivity should help us in our efforts to develop better ideas and solutions to security and defence issues for an increasingly complex global environment.

Statistically 25 % of ACT staff registered for the event and all available 2, 3 and 4 star Flag and General Officers participated as VIP Jammers. Additionally, our VIP Jammers contributed to 5 of the 8 forums and our staff posted in all; compared to the 2010 event where NATO was responsible for 4 % of the posts, this time it was 14 %. As such the interest the event generated within the organisation is self-evident.

To enhance this experience our staff were given free rein to comment as individuals, i.e. beyond ensuring they were aware of security constraints there was no ACT party line given for them to tow. Success or not? The statistics above demonstrate that two of our objectives were definitely met. The number of our staff that participated, together with the cross section of forums in which they contributed, ensured the educational opportunity was achieved as well as demonstrating ACT's desire to enter into debate on a wide scale. With respect to the report's recommendations, we are currently in the process of reviewing these in detail however, it is safe to say that there are some interesting ideas that require further investigation. What we certainly take from the event is that in principle it presents a unique opportunity to investigate and discuss with a wide cross section of subject matter experts issues that we deal with on a daily basis.

**Adm. Carol M. Pottenger**,
Deputy Chief of Staff Capability Development, NATO Allied Command Transformation (ACT)

ACT

*For national security policymakers, knowing 'who is to blame?' can be more important than 'who did it'?*
**Jason Healey, Atlantic Council of the United States**

The Atlantic Council's **Jason Healey** similarly believed that the so-called 'attribution problem' – whereby the exact source of a cyber-attack is difficult to ascertain – need not shut down global diplomacy in this domain. 'Attribution becomes far more tractable when approached as a top-down policy issue', he explained. 'If nations can broadly be held responsible for major attacks originating from their territory, then you are already well on the way to having "rules of the road", Healey added.

Jammers thus felt that global regulations were both desirable and possible in cyber-space. However, they were also realistic, and noted that such a big step will take a significant amount of time and effort to organise. Their recommendations thus focused on a series of interim steps (See Jam Rec. 6), and the search for 'lowest common denominator' policies for international actors, to help develop this new form of security partnership.

**Vytautas Butrimas**, Chief Adviser for Cyber Security at the Lithuanian Ministry of National Defence, was one advocate of this approach. He suggested that by focusing on bare minimum standards, such as accepting liability for cyber-activities emanating from within your borders, states could build confidence and trust in each other.

'Emphasis should be placed on the state's obligations to investigate and react to incidents originating from their own territory', Butrimas opined. 'Nations should ensure for example that ISP's take appropriate steps against individuals and/or information and communication technology equipment participating in a cyber attack'.

**Patrick Pailloux**, Director General of the French Information Security Agency, pointed out that simply having a known point of contact for cyber issues in every state could also be a 'quick win' option. This 'does not mean that you cooperate deeply with everybody. You're simply sure that if you have a question, a problem; a doubt... there is someone to call'.

With characteristics similar to the 'confidence building measures' used in conflict scenarios, Jammers therefore identified the groundwork that would be required for global actors to cooperate on an eventual cyber-space treaty.

However, not every partnership opportunity in cyber-space need focus on grand state-to-state diplomacy. Many Jammers focused on the inter-sectoral aspects of cyber-space, and the need to coordinate law enforcement, intelligence, industry and military actors to build more robust cyber-security.

As **Rob Wainwright**, Director of Europol, explained from his agency's perspective, 'the name of the game is collaboration'. He described how inter-connections between Europol, U.S. agencies and EU member state Computer Emergency Response Teams (CERTs) are allowing a new approach to the challenges of cyber-crime.

As such an example illustrates, beneath the grand scheme of a global cyber-convention, a whole host of new partnerships must be developed to advance a comprehensive cyber-security regime.

# 2. Developing the right tools for 21st century security

## The future technology needs debate

Jammers were intensely interested in a fundamental question of defence and security policy: what equipment will EU and NATO member armed forces need to meet the most probable upcoming security challenges?

This involved identifying the type of military roles Western nations anticipate for the coming years. Here, Jammers often found themselves caught between reflecting on the long and often painful experience of large-scale NATO-led nation building and counter-insurgency in Afghanistan, and Libya in 2011 – where air assets alone proved sufficient. Which best represents the military priorities for the future?

Generally, there seemed little appetite for serious discussion about future land interventions in the mould of Afghanistan. Indeed, infantry or armoured vehicle technology needs featured almost nowhere in the 2012 Security Jam. As **Dennis Prange**, defence analyst noted, 'NATO will be hard pressed to imagine a need for major conventional ground assault capabilities' any time soon.

Jammers had no interest in boots on the ground.

Instead, they focused on a range of power projection tools they thought would be the most relevant in the emerging global security environment. This included a discussion on Allied air power performance in Libya. Mirroring general opinion, **Shaun Waterman**, a reporter for the Washington Times, pointed out the obvious deficiencies in European intelligence, surveillance, target acquisition and reconnaissance (ISTAR) and Air-to-air refuelling assets.

'I think it is generally true that – though the Libyan mission was well-executed – it also drew attention to some of the ways in which NATO relies on unique U.S. capabilities', he explained.

This boiled down to a 'shopping list' of airpower capabilities which Jammers agreed European Allies in particular lacked in sufficient quantity or quality. **Admiral James Stavridis**, NATO Supreme Allied Commander Europe, highlighted AWAC command and control aircraft and other ISTAR capabilities on his wish list for NATO. Jammers were also enthusiastic about the potential of un-manned aerial systems (UAS) to help bridge current capability gaps in conventional air power.

Another area of strong interest was maritime technology. As one Jammer opined, 'NATO's maritime capability is well poised to provide the alliance a "quick win" in capability development.' (See Jam Rec. 1) There was certainly a feeling that in light of U.S. defence budget cuts, European navies may be called upon to do more for global maritime security, and that NATO should begin planning for this eventuality.

As **Eleni Ekmektsioglou**, Non-Resident Research Fellow at the CSIS Pacific Forum, explained, 'the U.S. is going through a "redefinition" period, and its Navy is exhausted and about to experience decommissions'. In this context, European allies cannot rely on the U.S. navy to always be available for small-scale operations such as anti-piracy.

**Rafal Nedzarek**, of the University of Liverpool, agreed. 'Ideally, the EU should set itself a mid-term goal to go beyond protecting its exclusive maritime interests and to relieve the U.S. of some of its burden', he said. 'This would enable the U.S. to intensify its commitment in the Pacific and in the Indian Ocean'.

To achieve this, **Magnus Nordenman**, Deputy Director of the Program on International Security at the Atlantic Council of the United States, recommended a range of technology needs for littoral (or 'brown water') and maritime patrolling roles. He claimed the Alliance 'should consider how it can enhance maritime domain awareness, integrate unmanned systems into naval operations, as well as consider platforms that can remain on station for an extended period of time'.

Op-ed

# U.S. European Command

Congratulations to everyone who participated in the Security Jam 2012! It is often said that 'No one person is as smart as all of us thinking together' and this year's Jam proved that point. At Headquarters, United States European Command we pursue our vision of 'Stronger Together' on a daily basis.

That's why we fully support these types of initiatives. Naturally, recommendations that enable all of us to work better together are fully in line with our philosophy. For example, Leo Michel's evolution of the idea of an International Community Planning Forum; a real brick and mortar place where practitioners from all the sectors involved in crisis and disaster response and post-conflict stabilization efforts could meet regularly BEFORE an event.

Getting to know one another's methods, cultures, and capabilities in advance of taking action, developing ways to better improve our cooperation, and building a common approach to collective effort, an approach in which each actor is afforded the best possible chance for success, is the epitome of our motto: Stronger Together. Our headquarters works with our military partners on this challenge every day. Increasingly, we are working with willing civilian partners as well. For example, our Joint Inter-Agency Counter-Trafficking Center, or JICTC, is working to bring the comparative advantages of military and civilian partners together for the common good. Their focus on transnational threats today will help us avoid bigger challenges tomorrow.

How we work together is the engine for what we are working on. The Security Jam is a great example of how to work together. It's an engine for progress, but only if we take up the challenge of implementing the recommendations; the challenge of moving forward. In an increasingly uncertain world, our ability to work together will be tested again and again. Our ability to respond is tested regularly in crisis after crisis. We are very good at it. Our ability to work together is less well developed. As the stakes rise and the resources to respond fall, our ability to leverage one another's efforts and advantages will be vitally important to our future success. The time to prepare together to work together is now. Our headquarters stands ready in many ways to join willing partners as we prepare together for an uncertain future. We each have strengths. Together we will be stronger... stronger together.

**Mike Ryan**, Deputy Director, Policy, Strategy, Partnership and Capabilities at the U.S. European Command

EUCOM

Future Capabilities and Technologies was the busiest forum in the 2012 Security Jam.

cooperation

alliances

cyber security

Others agreed that, given budgetary constraints, European navies should focus on niche capabilities that can complement the U.S.' continued carrier fleet supremacy such as anti-mine and maritime surveillance technologies.

However, other Jammers cautioned that this view of maritime security technology may be ignoring an important global arms trend: area-denial anti-ship missiles. Referencing the proliferation of anti-ship missile systems being pioneered by nations such as China and Iran, Prange predicted a shift in emphasis of maritime systems in the comings years.

'If the evolution in missile technology proves to be consistently more rapid than that of the countermeasures (historically a relatively safe bet) and produces 'game-changer' [technology] more often', Prange explained, 'credible power projection will be difficult'.

Jammers were thus cautious about prescribing specific numbers of platforms or systems necessary for securing the world's oceans, and acknowledged more research is needed. They did nonetheless agree that the rise of South-East Asian naval powers such as India and China would likely complicate NATO's role in the maritime domain in the coming years.

## Non-state threats to international security

Alongside military technology needs, Jammers explored a host of non-state security threats that they believed will impact global security, and suggested NATO and others need new doctrinal concepts to manage them.

Jammers generally condemned of the concept of the Global War on Terrorism as a militarised strategy. Instead, many called for a more sophisticated understanding of the connections between organised criminal gangs and terrorist groups around the world.

Positions varied on this. 'Terrorists use organise criminal structures and methods to finance their activities and criminals use terror to intimidate', said one Slovakian Jammer. 'It is crucial to change the narrative... and treat them as one joint threat'. However, **Benoît Gomis**, Research Analyst in International Security at Chatham House, countered that 'their goals are very different: economic gain for organised criminal groups and political, religious or personal statement for terrorism'.

Between these extremes, others assessed the linkages between regional instability and non-state actors. **Ian Anthony**, Research Coordinator at SIPRI and Director of the Programme on Arms Control and Non-proliferation, pointed out that this is particularly true in Somalia.

'In recent times, Al Shabaab (the Islamist organisation that controls much of central and northern Somalia) has been the nearest thing to a government in place, as well as an insurgent force', he explained. Anthony thus pointed out that as 'it has been willing and able to use terrorist tactics', and as Al Shabaab is now understood to be permitting the growth of Somalia-based piracy, this constitutes a combination of security problems that cannot easily be distinguished.

This understanding fed into a heated discussion on the concept of 'hybrid threats'. **Roy Hunstok**, Norwegian Army Brigadier General and Co-Chairman of the Deployable Joint Staff Element at NATO ACT, explained that the Alliance is increasingly focused on hybrid threat actors which cross borders, and defy existing categorisation as a defence, security or law enforcement threat.

Hybrid threats 'go beyond conventional weaponry and proliferation and now include clear links between piracy, cyber terrorism, threat finance, trafficking and social networking by non-state actors and terrorists', he explained.

## Op-ed

# Atlantic Council of the United States

With the 2012 Security Jam now behind us I have had a bit of time to reflect on the outcomes and how they can be taken forward. Below follow my observations:

**Outcomes**

In my mind the recommendations coming from the Jam were somewhat surprising, and also provided an interesting data point on where the national conversations are when it comes to NATO, the EU, and the transatlantic community. It is clear that people have moved on from Afghanistan, and now wants the transatlantic community to focus on emerging challenges, such as cyber defense, soft security issues, maritime security, and NATO's role in the Middle East following the Arab Awakening. Furthermore, judging by the dialogue during the Jam it is clear that most participants view the NATO Libya operation as a template for future NATO operations, rather than the Afghanistan effort. The wider security community should pay attention to this shift when formulating policies and constructing outreach campaigns, since this is where the interest in transatlantic security is currently focused.

With this context, a few wave tops stand out as key take-aways from the Security Jam.

1. The logjam in the NATO-EU relationship persists, and impacts the transatlantic community's ability to plan for contingencies, wisely spend scarce resources, and to undertake concerted efforts. This is of course not a new theme, but it is a fundamental one in urgent need of a fix.

2. Partnerships in all its dimensions. A common denominator across forums and themes is the need for partnerships between organizations such as NATO, and actors ranging from industry (for generating and sustaining capabilities) to emerging nations such as China.

3. Participants of all stripes and backgrounds are acutely aware of the age of austerity, coupled with a perception of the US turning away from Europe and towards the Indo-Pacific region. A real effort is needed to sustain the transatlantic security relationship in light of these developments.

**Next steps**

It is important that the deliberations and key themes that emerged during the Jam are captured by the organizations involved. This can be done in at least two ways:

- A review in a year on "where are we now?", which would include looking at where the issues stand today, and if there has been any movement on them. Were the jammers totally wrong on some predicted world development? Were they completely right on something? This may also serve to further validate the concept of the jam.

- The participating organizations should seek to integrate the findings and themes of the Jam into current and future programming.

**Magnus Nordenman**, Assistant Director,
International Security Program,
Atlantic Council of the United States

Atlantic Council

**Op-ed**

# Chatham House

The 2012 Security Jam provided a timely opportunity to tackle many difficult cyber security questions. Numerous discussion threads focused on broad and far-reaching issues, such as opaque terminology, immature governance models and a lack of human talent and leadership. There was also debate over the nature of threats in cyberspace as well as the range of appropriate response mechanisms. The general consensus was that, when discussing cyber security, questions outweigh answers by an order of magnitude.

Cyberspace challenges existing norms and traditional concepts of security and defence. Although the current absence of clarity and consensus can be frustrating, it seems appropriate given the evolving and expanding nature of the cyber domain as well as the multitude of actors and their deeply rooted inter-connections and dependencies. Cyber security may represent the defining security challenge of the early 21st Century, and the Security Jam provided a valuable space for discussion and debate. There was a desire among participants to address difficult questions and develop more nuanced policy approaches. The action-oriented focus of the forums was particularly notable, and served to bridge the gap between a multitude of questions and a handful of answers.

Improvement in many aspects of cyber security is highly dependent on political will, and on the ability of decision-makers to grasp the importance and ramifications of the decisions they face. Improvement is also reliant on accurate measurement. What metrics will the public and private sectors use to judge success or failure in cyber security, set benchmarks that can make meaningful contributions, and develop and preserve the institutional memory necessary to innovate and improve cyberspace over the long term?

Above all, cyber security should be viewed not as an end in itself, but as a means to an end. Although cyberspace presents new risks it also offers myriad opportunities, and should be seen as an enabler for the continuing social, economic and political goals that all nations wish to achieve.

**Claire Yorke**, Programme Manager and
**Dave Clemente**, Research Analyst, International Security Programme, Chatham House

*Hybrid threats are hammering us... and draining our economy as we speak.*
**Roy Hunstok, NATO Allied Command Transformation**

In Hunstok's view, the Alliance needs to develop a doctrine for understanding the complex challenges raised by groups such as Al Shabaab, Al Qaeda, hacking groups such as Anonymous or global terrorist networks with no clear command structure. 'We have a huge challenge as long as we have no policy or concept', he lamented.

Others focused on how new combinations of hostile non-state actions could be combined to create hybrid security challenges. Dubbing one such threat 'geo-weaponeering', **Cheryl Durrant**, an Australian civil servant, explained how the simultaneous deployment of an un-conventional cyber or terrorist attack with a natural disaster could lead to a vast multiplication of the potential damage.

'This is a relatively new concept for the military legal field,' she explained. 'Most of our legal research so far has focussed on the applicability of current laws of armed conflict... to cyber and information operations, not to the use of geo-weaponeering or environmental factors'. By effectively harnessing the effect of natural disasters, hybrid actors could gain a cheap force multiplier through geo-weaponeering, a serious concern for some Jammers.

## Europe's 'pool it or lose it' moment

Underlining all of these discussions was an acute appreciation of the urgency to share military equipment imposed by the current financial crisis. Some Jammers even extended this priority to civilian crisis management equipment. (See Jam Rec. 8).

In the defence arena, attention turned to Europe, where Jammers were unanimous in acknowledging that new levels of cross-border cooperation will be needed if European states are to maintain any meaningful defence capacity.

**Claude-France Arnould**, Chief Executive of the European Defence Agency, explained that pooling and sharing (P&S) military equipment will require a combination of regional and pan-European partnerships. Arnould noted ongoing European initiatives to pool and share air-to-air refuelling aircraft, helicopter training and field hospitals that serve as examples of this cooperation already in progress.

Such structures should not be based on the size of the nations involved, but the urgency of the operational need for equipment, she explained. Thus, 'on some of these actions, big member states took the lead; on others, such as naval training and maritime surveillance, smaller member states play a key role. Progress will be obtained by the combination of these impulses'.

However, other Jammers painted a less optimistic picture, pointing to the on-going challenges of convincing member states to relinquish sole control of their dwindling military assets. As **Giles Merritt**, Director of the SDA, succinctly put it, 'fear of the loss of national sovereignty is still the main obstacle to progress'.

This question boiled down to matters of national interest, with Jammers keen to find ways to fit the obvious budgetary need with national concerns about sharing equipment with neighbours.

*NATO's Smart Defence and the EU's initiative for pooling and sharing complement each other. We must not duplicate each other's projects.*

**Ton van Osch,**
**European Union Military Staff**

**George Harnett**, a financial sector risk analyst, was realistic about this, arguing that national concerns about sovereignty should not be bemoaned, but instead integrated to the P&S process. He wondered, 'would it be more productive to develop a framework for bilateral or multilateral co-operation based on mutual interest… rather than trying to develop a grand framework of sharing and inter-operability that would require some nations to act outside or even against their national interests'?

Jammers were generally supportive of this idea, though the potential groundwork for this European 'mutual interest' at times seemed elusive. As Ekmektsioglou noted, there is a risk amongst smaller nations of finding themselves entirely dependent on European neighbours for their defence. In certain situations, 'states would easily prefer less power to dependency', she warned.

**Jonathan Dowdall**, a Brussels-based defence and security affairs journalist, offered one suggestion to overcome this, by focusing on the tasks particular assets can undertake. 'Individual national interests may change, but the assets required to address particular problems change less so', he said, noting for example the general usefulness of equipment such as strategic-lift aircraft for deploying forces.

'If Europe can decide which tasks it needs to fulfil, and prepare pool and share frameworks to meet those, even if interests change, the assets will remain broadly relevant' across time, he explained.

Others felt the entire 'sovereign assets' debate as dangerously obstructive to progress. **Pauline Massart**, Senior Manager at the SDA, pointed out that it 'is now extremely short-sighted in a modern perspective: no single European nation today has the capabilities to defend itself, and as we all know, the financial crisis will only make the situation worse'.

Here, Jammer opinion strongly mirrored the call by SACT General Stéphane Abrial that European military staff need a new 'mindset' for defence collaboration. (See Jam Rec. 4).

In light of this, Massart challenged the nationalistic overtones of the sovereignty debate. 'It is unpatriotic today to promote national interest over a common approach in security issues'.

Op-ed

# Fondation pour la Recherche Stratégique

The vast virtual brainstorming allowed by the one-week Security Jam has been particularly useful in identifying the multiple facets of the theme 'international cooperation in capabilities'. Notably, the forum highlighted duplication of capabilities between the EU and NATO (both push for Pooling and sharing / Smart Defence initiatives), the scope and impact of the U.S. shift toward Asia, the rationale of such cooperation and how to improve it (through doctrine or training for example).

European militaries are condemned to shrink as the economic crisis supersedes all strategic stakes, by essence limited by the absence of vital military threats and the rejection by most Europeans of the idea of strategic power which uniquely underpin any military construct. In such circumstances, M&S/SD is appealing. Why then is the vigor of the debate only matched by less than convincing results? The reason seems twofold:

On the one hand, the lack of compelling threats and the comfortable insurance of U.S. military and, as a consequence, the low ranking of defence matters on political agendas;

On the other hand, the remaining divergence between European partners regarding not only their strategic and economical interests and priorities, but also their strategic cultures and the related level of military interventionism, as Libya once again demonstrated.

The situation prevents multilateral frameworks from going beyond the lowest common denominator of defensive capabilities, such as air defense, and the supporting ones, including space enablers, air mobility assets, or search and rescue capabilities, areas where M&S/SD is already a reality.

For more sensitive and combat capabilities, cooperation between military institutions and the associated painful decisions regarding capabilities or industry require a true shared political will that is precisely lacking in the current context. In other words, as history of the last decades demonstrates, M&S/SD works only when the strategic context leads political leaders to actively build something together. This condition is necessary but not sufficient: beyond political will, international cooperation is built up on the right balance and concomitant interest among military and industrial spheres. Past cooperation programmes show that the three spheres are equally important and must be satisfied for successful cooperation.

Considering this first condition for success in international cooperation, frameworks for cooperating are a secondary but still important issue. Beyond multilateral frameworks (NATO, EU) and bilateral initiatives (UK-French agreement, for instance), the EU provides another framework (notably, permanent structured cooperation), which has the merit of being more European than a bilateral agreement and flexible enough to avoid the blockage of 27 different defence cultures, interests and needs. This tool could be exploited to develop cooperation on a regional basis, for instance, or among interested countries.

▸▸ **Philippe Gros** and **Marta Lucia**,
Research Fellows, Fondation
pour la Recherche Stratégique

FRS

Op-ed

# The Hague Centre for Strategic Studies (HCSS)

**The Libya litmus test?**

From the perspective of the mandate given to NATO by UN Security Council Resolution 1973, NATO's intervention in Libya was a resounding success, exemplifying its continued relevance in the 21st century. However, from a broader perspective, it might be too early to judge the lasting effects of this intervention, both for Libya and NATO. One cannot help but wonder if the present state of the country will create a 'better peace' for the Libyan population. Arguably, the backlash against perceived old-regime supporters, the current infighting among militias, and the proliferation of small-arms in the region had not been properly anticipated. Lasting effects would have required insertion of peacekeepers and non-governmental organisations to help stabilize the nation. However, oppositional forces in Libya made it clear they did not want foreign assistance on the ground. With the exception of a few special forces to direct air strikes, that has indeed not happened.

The only conclusion that does not seem premature is that interventions within a 'Responsibility to Protect'–context (R2P) require more critical thinking in advance. Although NATO respected its mandate, the desire to remove Gaddafi may have caused mission creep, stretching the political intention of the UN-resolution. This may have caused Russia and China to regret their abstention on this resolution. Additionally, NATO's operational success could have given Russia and China a thorough scare. Whatever the real reasons for their present policy, as a regrettable result, it could be much harder to obtain a UN-mandate for future interventions under the rubric of R2P.

The UN/NATO-actions in Libya and the inability to intervene in Syria may also have strengthened some nations' perception that R2P is used for Western interests. To address this perception, a debate has to take place on a realistic future for R2P, especially within the UN. The initiative of 'Responsibility while Protecting', recently revitalized by Brazilian President Dilma Rousseff, could be an interesting addition to this debate. An effective R2P-concept is imperative, not only to deter current regimes to commit atrocities, but also as a template guiding decisions on future interventions.

The good news is that 'Unified Protector' has shown the alliance's capacity to act. However, only a limited number of NATO members actually participated, due to the controversial nature of the intervention. Several NATO members abstained from voting in the North Atlantic Council, while allowing others to proceed. It is not yet clear how this has damaged relations between NATO-members. It could mean the concept of Smart Defense is in jeopardy, as it is based on mutual trust. The operation in Libya revealed serious capability gaps. Whether 'Chicago' made an important step in solving this, remains to be seen. There is too much unfinished business from 'Lisbon' to attend to.

**Joris van Esch**, Strategic Analyst,
Comprehensive Security Program,
The Hague Centre for Strategic Studies (HCSS)

> *Defence procurement bureaucracies are still condemned to working in the strait-jackets of the age when innovation happened in decades, not years.*
> **Klaus Becher, International Technology Consultant**

## New industrial structures for a healthier defence outlook

Underpinning all of these suggestions ran a debate about the future structure and composition of the European defence sector. Jammers were in agreement that, especially as the global economic situation recovers, industrial policy will be an important element of the future defence environment. (See Jam Rec. 3) They also argued that national agencies, NATO and the EDA will need to proactively engage with industrial issues to advance security policy.

As **Lucia Marta**, Research Fellow at the French Fondation pour la Recherche Stratégique noted 'industrial capacities are key national assets from the economic and technological point of view, and are the symbol of national prestige and independence for the implementation of their defence policy'.

Many Jammers agreed that projects such as Smart Defence can only succeed if the likely ramifications for national defence industries are adequately included in the cost-benefit calculation.

Others called for a change in the way industry engages with both NATO and ministries of defence when developing new technologies, claiming that the current system of contract tenders, competition and procurement is proving too slow.


**Leendert van Bochoven**, NATO and European Defence leader at IBM, explained that there 'is a need to coordinate with industry, and make sure that NATO speeds up the cycle of interacting with industry in this domain'. Adding that 'organisations like ours have to go through a series of research questions in order to determine where we make our (long term) technology investments', van Bochoven advocated for a more strategic vision of long-term equipment goals.

Other Jammers agreed that new models of defence contracting should be used more widely, such as 'Pre-Commercial Procurement' or 'Pre-Operational Validation' – processes whereby the risk to industry of developing and testing new technology is offset by a public buyer guarantee to utilise the resultant product.

As International Technology Consultant **Klaus Becher** advocated, this would help move prototypes into service more quickly. 'What would help is to invite creative engineering teams to develop and build quick low-cost solutions, test these in an operational environment and then decide which defence-specific additional requirements need to be added on top of the proposed solution to bring the equipment into service', he said.

By building these new industrial relationships, industry and NATO can more readily identify which technologies will be needed to underpin Alliance member military ambitions. Jammers agreed that such public-private cooperation holds the potential for a generation of new military equipment to be delivered rapidly and cost-effectively.

Op-ed

# Konrad-Adenauer-Stiftung

The end of the allied Afghanistan campaign is drawing closer. With the combat mission to end as early as 2013 and the exit date being set for 2014, there is one clear message to Afghanistan, the region and the audiences in the allied member states: NATO is on its way out. Yet, political leaders in the West continue to argue that the alliance might withdraw its troops, but will remain invested in Afghanistan and do all but abandon the conflict-ridden state. With NATO set to withdraw, Afghanistan and Pakistan on the brink, and an all but beaten Taliban one is led to wonder what exactly allied leaders plan to live up to that promise?

Would it not be such a relief to finally have a timetable for the exit of allied forces, the West's political leaders would be pressed for a strategy for January 2015 and beyond. The timetable is even more pressing than the arbitrary timeline suggests. With forces leaving the theatre, it will become increasingly difficult to influence events on the ground and if the alliance wants to adjust course it has to do so right away. Such a shift in strategy needs to take a careful look at three areas in particular, if it wants to be successful. It needs to reach out to the larger international community and foster governance reform with a much larger focus on facilitating educational programmes.

While NATO is trying to hand over its responsibilities on the ground to its Afghan partners, it also needs to ensure that it internationalises its efforts and reaches out to the United Nations and the Shanghai Cooperation Organisation (SCO). The United Nations already maintains a small support mission in Kabul and could – given that the West musters the political will – be expanded to help guide the Afghan government through a difficult transition period. Though a successful end of the Afghanistan campaign is in the vital interest of the West, it is also undeniably an even more important interest of Afghanistan's neighbours and NATO should begin to convey that message to Afghanistan's neighbours and regional organisations such as the GCC and the SCO.

While Western leaders maintain that the Afghan state needs to improve its governance performance in order to dry up the Taliban insurgency, rampant corruption, a drug economy and lack of transparency prevented such progress time and again. In fact, corruption and the constant focus on administrative capacity has led the international community to neglect an issue as important as capacity: legitimacy. Election fraud, corruption and the willingness to undermine local authorities in favour of short term security gains have eroded the legitimacy of the Afghan state and the Afghan campaign. Repairing the damage done by this negligence requires another long-term commitment and NATO needs to commit the resources necessary right now. But it also needs to recognise that the one area that is a prerequisite for overall success is education.

NATO's withdrawal will make the formulation and execution of an Afghan strategy more difficult than it already is. The alliance might have one last chance to change course in Afghanistan. If it wants to enter 2015 fully prepared that time is now.

▸▸ **Dustin Dehez**, Member of the Standing Group on Foreign Policy and **Julian Voje**, Young Foreign Policy Experts, Konrad-Adenauer-Stiftung (KAS)

*The concept of 'comprehensive approach' in the EU crisis response/management cycle is not new, but it is high time to fully implement it.*
**Agostino Miozzo,**
**European External Action Service**

# 3. Sustaining knowledge and expertise in new fields

## Fostering careers in security

Jammers were also interested in the human elements of security policy – specifically how to manage specialist expertise and knowledge in civilian fields such as crisis management and cyber-security.

A great deal of attention was given to the European External Action Service (EEAS) in this area. Jammers were interested in how this relatively young EU branch can better integrate the experience of its field mission staff within the more general Brussels-based career path. (See Jam Rec. 8)

One recent development within the EEAS enthusiastically discussed by Jammers was the creation of the EU Crisis Platform. Aimed at better coordinating the designation of scarce human resources for crisis management, the platform brings together various existing EU crisis response/management structures under one roof, in coordination with DG ECHO, the Commission's humanitarian assistance branch.

As the architect of the new structure, **Agostino Miozzo**, Managing Director for Crisis Response and Operational Coordination in the EEAS explained, 'we should not try to reinvent the wheel every time. What we are trying to do at the EEAS is to improve our crisis response capability by better using all the existing instruments, in a targeted and efficient way'.

As well as permanent structures within the EEAS, Miozzo also noted the importance of temporarily seconded staff from Member States in handling crises such as Libya. 'Staff deployed temporarily do play a coordination role that is much appreciated', Miozzo explained.

Indeed, others felt that the use of temporary secondment was not being adequately factored into personnel development. **Hylke Dijkstra**, a postdoctoral researcher at the Department of Political Science of Maastricht University, was one advocate calling on the EU to better ensure 'that foreign experience does not decrease career prospects'.

Noting that time in the field is not often integrated well into the average EU career, Dijkstra urged 'member states to think much harder about the career paths of their personnel. This not only goes for the civilian staff members, but also for example national diplomats seconded to the EEAS... These people come back and they deserve a promotion'.

This was deemed particularly important for specialist fields, such as security sector reform (SSR) in post-conflict scenarios. **Giji Gya**, Head of the Deputy Director's Office, DCAF, said more time abroad should be factored into this sector's career path. 'Strengthening (for SSR) Member State capacities for training - and harmonising of such, e.g. through turning the ESDC European Security & Defence College - a virtual frame that uses Member State training capabilities - into a body with capacity in its own right - as well as creating a comfort zone for personnel career development (and a return to careers in their member states after working abroad) is very important too', she affirmed.

In a time of financial constraint, other Jammers focused on the need to better mobilise under-exploited human resources in the military. **Frédéric Jouhaud**, incoming General Secretary of the Interallied Confederation of Reserve Officers (CIOR), argued that Europe's infantry reserves should be mobilised more for crisis situations.

'The reserve forces capabilities in some domains like education and health... offer a credible and value asset to EU and NATO to extend their actions, and to participate [in roles such as] border security,' he said.

> *The essence seems to be the overall lack of cyber-security talent.*
> **David Clemente, Chatham House**

This idea was not universally supported, however, with one military Jammer noting 'that European reserve forces are too few, untrained and unavailable'. **Jack Clarke**, Professor at the Marshall Center and Director of their Program on Civil Security, was also sceptical about their capacity to deploy, adding that 'in many European countries, reserve forces are less than 10% of their Cold War numbers'.

In cyber-security, Jammers were greatly concerned that key actors, especially national authorities and the EU, were not adequately staffed with competent cyber-security professionals. As **David Clemente**, Lead Cyber Security Researcher at Chatham House, pointed out, the 'pool of highly skilled people is small, [and] it is expanding steadily, but linearly, while cyber threat vectors are proliferating at an exponential pace'.

This urgent skills deficit spurred some controversial ideas – such as potentially expanding the recruitment of former hackers into the public sector cyber-security community. (See Jam Rec. 7)

**Adam Sadowski**, a Polish International Relations student, argued that such schemes could also help transform the 'mindset' of hacker groups. 'Backed with a decent salary and good 'propaganda' (ie. the creation of some kind of 'mission' feeling), this could help to attract talented youth, and perhaps even some on-line veterans', he claimed.

An expansion of general ICT education programmes at both pre and post-graduate level was also deemed urged. As **Burkhard Theile**, a defence industry analyst argued, the 'most important element is systematic training and qualification: there are too many people who have a perception of the problem, but probably do not even know how a data package travels around the world'.

Whether in cyber-space or post-conflict environments, Jammers were keen to better exploit developing talent in Europe.

Op-ed

# Stockholm International Peace Research Institute (SIPRI)

Transnational and hybrid threats: Modernizing our definition of security.

What does it mean to be secure? At the periphery of Europe and in contiguous regions the effects of conflicts of a traditional kind can be felt across the continent. However, few Europeans worry about being invaded by a foreign army or being attacked by armed bands in their own country.

It is becoming normal to see the citizen, rather than the state, as the point of reference for security. A modern definition means protecting the things that individuals hold dear – both tangible (person, property and possessions) and intangible (lifestyle, freedoms and values).

Securing citizens against non-military threats may be beyond the capacity of national authorities. For example, citizens are under threat from terrorists operating within their own society who may have been previously unknown to the national authorities, those that come from the outside or a combination of the two. Organized economic criminals operate in the expanding electronic market place, but their location may be unknown or beyond the reach of national law enforcement. Traffickers exploit transnational networks to move drugs, people and weapons to customers and to launder money.

In an internationalized and increasingly globalized economy, businesses and people change location more often and to more places, and citizens depend on international flows of money, goods, materials, energy and ideas. Access to these flows is considered normal and the political impact of loss of disruption is magnified.

Things that citizens value are often outside direct state control. Private companies provide us with jobs, houses, electricity and transport and operate critical infrastructure in a modern society. They play an important role in providing health care and education. Private companies and other non-governmental bodies must play their part in building security.

The discussion of transnational and hybrid threats in the SDA Security Jam underlined how complicated and sophisticated future security policies will have to be to meet the needs of European citizens. A much wider range of public bodies must now be engaged, including financial authorities, the law enforcement community, public health authorities and a broad range of regulators. These authorities often have little experience of cooperating. New partnerships will have to be forged with private bodies that have no experience of working with security issues (or considering themselves as part of the security community).

Integrated and holistic approaches should be sought and promoted to categories of transnational threat – such as organized crime, terrorism, trafficking or piracy. It is obvious that cooperation is a critical element in addressing transnational and hybrid threats, but a better understanding of how to construct and manage the complicated networks needed to promote and implement effective cooperation is needed.

To reduce the risk that integration could be a destabilizing factor and promote transnational threats more attention must be paid to e.g. effective enforcement of measures to tackle corruption, trafficking and other forms of organized crime prior to or in parallel with integration processes.

**Ian Anthony**, Director,
Arms Control and Non-Proliferation Programme,
Stockholm International Peace Research Institute (SIPRI)

SIPRI


## 'Open sourcing' security?

Perhaps unsurprisingly in an online forum, Jammers were interested in the potential for web-based services and 'crowd-sourced' knowledge to support security and defence policy.

As well as advancing the idea of an e-learning based education scheme to support Afghan security post-2014 (See Jam Rec. 5), Jammers were intrigued by the potential for online sources to pool valuable knowledge and expertise for crisis management. (See Jam Rec. 9)

As **Marco Overhaus**, Senior researcher on European Security and Defence Policy at the German Institute for International and Security Affairs explained, open-source efforts of this kind can help move operational expertise a step closer to policymakers. Overhaus suggested that 'every ministerial meeting be preceded by an "information summit", which would be in turn preceded by online open-source consultations, systematic exchanges with academia/think tanks, round-tables, seminars and so forth'.

However, others noted that simply collecting information online is not enough – you have to adequately filter and process the information to make it operationally useful.

As **Jorge Benitez**, Senior Fellow at the Atlantic Council of the United States explained, 'communications technology is the most promising answer... The key challenge is data management, which is to say, identifying the information that is most relevant and valuable'.

'The critical filters necessary to provide operational value to data management are contextual and direct experience,' he added, suggesting that whilst 'open-sourcing' is a valid idea for some security areas, a degree of expert moderation is still required.

An anonymous jammer cautioned the same, adding that 'the capabilities, organisation and resources needed to develop and maintain such understanding are not insignificant', and indeed, not necessarily cheap.

'Alliance member nations may have to overcome significant inertia if they are to achieve the insights the future security environment demands', they concluded.

One of the more technology oriented open-source ideas proposed came from **John Parks**, a marine scientist, who raised the idea of a 'wiki-maritime-surveillance' system – whereby the numerous radar, sonar and camera feeds used by shipping around the world could be pooled into an online, live-data depository.

Such a system, available for both private, coast guard and military actors to access, could greatly assist in alerting authorities to pirate attacks, vessels in distress or abnormal weather. 'Such efforts are already getting underway in an ad hoc manner', Parks said, adding that such a system 'could greatly benefit from international coordination and standards setting efforts'.

Though many cited technical obstacles such as available transmission bandwidth and signal quality – as well as legal concerns over privacy – as such ideas illustrate the potential for security challenges to be solved through 'open-source' solutions.

Op-ed

# Stiftung Wissenschaft und Politik (SWP)

**Crisis Management in Crisis – From Cooperation to Division**

After the end of the Cold War crisis management developed – on balance – into a unifying concept which allowed member states of NATO and the European Union to cooperate in their security and defence policies even after bi-polarism had gone. In that sense, crisis management became a central rationale for the ongoing existence of Euro-Atlantic security institutions. Today, we may witness a fundamental change which could eventually turn crisis management from a cooperative into a divisive endeavour.

Since the early 1990s NATO has debated its role in 'out-of-area' operations – which take place beyond the defined treaty area and are not tied to collective defence – and put this new role in practice in the former Yugoslavia. The verdict '"out-of-area" or "out-of-business"' reflected the prevailing mood. The emergence of the Common European Security and Defence Policy (ESDP/CSDP) of the beginning of the 2000s was equally and almost exclusively tied to the notion of crisis management by civilian and military means.

True, there were fiascos early on, such as the one which occurred in Somalia in October 1993. Multilateral interventions in third states have always had their divisive elements such as debates about burden-sharing or about the proper role of the military. Yet, there are good reasons to think that this time more profound changes are taking place. These changes are likely to have a negative impact on the level of ambition and, more profoundly, on the ability of Western security institutions – and the 'international community' at large - to engage in multilateral crisis management.

First, the sovereign debt crises in the United States and most European countries are very likely to be a longer-term phenomenon. Both smaller and bigger countries have initiated significant cuts in their defence budgets. The amount of money available for foreign and development policies might eventually shrink as well. Coupled with an 'intervention fatigue', observable in many Western public opinions this is likely to lead to a much lower level of ambition and to more quarrels about burden-sharing.

Second, there is also the problem of declining legitimacy. It is by now common sense that the post-World-War-II international order, with the United Nations Security Council playing a crucial role, is declining. The 'emerging powers' are demanding their share but the contours of a new order are not yet in the cards. Against this backdrop, the disputes in the Security Council about the 'Responsibility to Protect' and the military intervention in Libya in March 2011 may just be a forerunner of international divisions to come.

These and other issues were also intensively discussed during this year's Security Jam, including in our forum on crisis management. For certain, the debate about the changing context and contours of crisis management is just beginning.

**Marco Overhaus**, Research Fellow, Stiftung Wissenschaft und Politik (SWP)

*The Libyan operation demonstrated that 12 years and more than 20 CSDP operations later, Europeans still failed to obtain the capacities they had for so long identified as needed.*
**Ana Maria Gomes, European Parliament**

# 4. Future policy choices in a decade of austerity

## 'R2P, or not R2P?' – Libya's problematic template for future intervention

When it came to the question of future interventions by Western militaries, as already noted, the touch-stone case study for Jammers was NATO's 2011 campaign over Libya.

Debate raged as to whether Operation Unified Protector's (OUP) combination of 'Europe-lead, U.S. supported structure, no boots on the ground and aggressive air campaign highlight a future model for low cost interventions in an age of austerity.

One area of interest was the political and diplomatic effort undertaken to forge the OUP coalition, and how this reflects on the health of the Alliance. Many noted with dismay the initial reluctance of key allies such as Germany to join actions over Libya, claiming this cast a dim light on the potential for common future deployments.

However, **Brigadier General Peter Sonneby** Danish Air Force Commander in the NATO Joint Analysis & Lessons Learned Centre, disagreed with this 'glass half empty' assessment. He pointed out that 'about half of the Allies did choose to engage', a remarkable achievement in the middle of a European financial and political crisis.

To Sonneby, this demonstrates that NATO can still be relied upon to mobilise a viable force structure at short notice. 'I perceive that this is a positive outcome, as even if Nations have reasons not to participate in an operation, it does not prevent the Alliance from taking action', he said. 'This bodes well for the future of NATO'.

Yet despite this, there was caution about using the Libya operation as a general example for future missions, with Jammers noting an array of specific contextual factors surrounding Libya in March 2011 that made it a viable operation. **Lorenzo Nannetti**, Chief Analyst for Middle East and European Affairs at Caffè Geopolitico, noted that 'elements combined to make it worthwhile and doable – these may not occur simultaneously again'.

Indeed, **General Knud Bartels**, Chairman of the NATO Military Committee and Chief of Danish Defence during the Libya operation was unequivocal on this front. He said that 'the unique combination of international support, political will, partnership and cooperation, and NATO's military capabilities in the geographic region, were all critical elements in the Alliance's successful intervention'.

'The Libya campaign is not a template', he added.

Another area of intense debate surrounded the 'responsibility to protect' (R2P) principle – the UN norm of intervening based on humanitarian grounds that led to the granting of a UN mandate in Libya. (See Jam Rec. 10)

Many insisted that the Libyan example has dangerously undermined the R2P principle. Noting a high degree of obstructionism in the UN Security Council from China and Russia since the Libya operation – particularly during on-going attempts to resolve the downward-spiralling Syrian security situation – some felt that R2P has been discredited due to the eventual removal of Gaddafi.

'Russia and China... are wary of repeating a Libya scenario because of their absolute opposition to regime change', **Felix Rathje**, International Relations Officer at the European External Action Service, claimed.

*NATO must be flexible, capable and ready to prevent a wide range of crises and conflicts in our dynamic and unpredictable security environment.*
**General Knud Bartels, NATO Military Committee**

transparency
flexibility

This fed into a debate on so-called 'lighter' R2P options for future intervention. As **Hylke Dijkstra** from the Maastricht University opined, 'R2P does not have to be full-fledged humanitarian intervention', but could instead be used to force parties to the negotiation table, or to otherwise stalemate violence for a political re-conciliation. The Brazilian-led diplomatic proposal of a 'responsibility whilst protecting' doctrine, with stricter criteria for interventions, could support such a concept.

'It seems therefore important to think of lighter scenarios in the context of the R2P that may be palatable for the other permanent members of the UN Security Council, and easier to carry out', Dijkstra observed.

Yet others cautioned that Western allies should not be complacent about the role of R2P in future policy. As one American Jammer noted, 'State sovereignty and the Chinese/Russian led rule of non-intervention is still very much alive, and probably stronger in much of the world than R2P'.

Sadly, 'Syria seems to provide proof of that, and its people are paying the price', he added.

R2P
crisis
management

## The future division of labour between the U.S. and Europe 'post-Pacific Pivot'

Running throughout all of these discussions was one fundamental fact – that in a time of budgetary austerity, the U.S. now expects its European allies in NATO and elsewhere to assume more of the global security burden.

With Jammer commentary on the new U.S.-Europe division of labour in areas such as maritime piracy and cyber-security policy already highlighted, some final discussions focused on how Europe would factor in to what many are calling China's rise towards an 'Asian century', and accompanying U.S. 'Pacific Pivot' in its defence posture.

**Philip Shetler-Jones**, Brussels based Europe-Asia security specialist, captured general Jammer consensus by pointing out that 'Europe's security institutions are largely absent from the Asian scene, and Europe continues to rely on the U.S.A to take care of its interests'. Lacking any major military bases or robust power projection capabilities in the region, the ability for European powers to militarily support U.S. policy in South East Asia was generally downplayed.

Indeed, whilst some suggested that the gradual expansion of the EU's Common Security and Defence Policy could eventually see EU military task forces operating at great distances from Europe, the huge equipment challenges facing Europe's current regional policy ambitions seem insurmountable enough without grand China Sea dreams.

As **Patryk Pawlak**, Research Fellow at the European Union Institute for Security Studies asserted, 'one needs to openly admit that the EU will never be a military actor in Asia; nor should it try to be. The past decade has clearly demonstrated the limitations on the European side'.

*Over the past two decades, we [NATO members] have developed a unique mix of hard and soft power instruments. Today, that mix is more relevant than ever. I am personally convinced it will become even more valuable in the future.*
**Alexander Vershbow,**
**North Atlantic Treaty Association (NATO)**

Instead, Jammers advocated that the EU should bolster its role as a civilian security actor in Asia, alongside the U.S.' growing military presence in the region. As Pawlak observed, the 'EU definitely has a lot to offer in a broadly defined field of security, especially when we talk about civilian crisis management. The EU monitoring mission in Aceh shows clearly that a geographical distance is not necessarily an obstacle'.

**Anil Sankar**, a Singaporean Jammer, agreed that Europe's normative values on the world stage have intrinsic strategic value. 'The Asia-Pacific region will see new rising powers in the years to come. Europe certainly has a role to play to shape behaviour, and bring these powers on board to the international system', Sankar said.

'The EU is a dominant voice in many international fora', he added, 'and can play a role in building a security architecture for rising Asian powers'.

Others agreed that, despite the U.S. shift in military emphasis away from Europe, the diplomatic functions of NATO will remain a valuable tool for global stability. **Major General Mark Barrett**, Deputy Chief of Staff for Strategic Plans and Policy at Supreme Allied Commander Transformation HQ, noted that 'the [2010] New Strategic Concept states that 'promotion of Euro-Atlantic and international security is best assured through a wide network of partner relationships with nations and organisations around the globe'.

Such NATO partnerships are about more than deployed military force, and include the confidence building and nation-to-nation diplomacy that Jammers noted as being so important in the new security environment. This power of outreach will not only be important with major powers such as China, but also with India, Brazil, Indonesia, South Africa and other rapidly growing economic and diplomatic actors.

Indeed, many highlighted the sizable 'soft power' assets – ie. the ability to influence through attractive values and cooperation – of NATO members that will help sustain its relevance, even in an 'Asian century'. As **Alexander Vershbow**, NATO Deputy Secretary General explained, such soft power is 'vital for dealing with global security challenges such as terrorism, proliferation and piracy'.

Adding that further developing NATO's global partnerships will be a 'key goal' at the May 2012 NATO Chicago Summit, Vershbow was thus clear that European Allies will have an important role to play in the coming years, despite their current military budget woes.

# V. In conclusion

The 2012 Security Jam was undoubtedly a resounding success, with Jammers from around the world using the opportunity to share their thoughts and promote new ideas.

Across the Jam's wide ranging discussion, there were a few final overall trends that may be interesting to consider.

## In with the new, but what about the old?

Jammers were enthusiastic about new ideas, structures or initiatives. As the Jam Recommendations and general debate illustrates, most wanted to propose the creation of new agencies, working groups or technologies to deal with today's security challenges.

However, Jammers seemed less able to distinguish which existing institutional structures they would like to see removed or discontinued. Equally, whilst the 'wish list' of future capability needs quickly grew to include a wide array of cutting edge technologies, few Jammers were willing to concretely say which capabilities they would like to see decommissioned amongst Alliance militaries.

It seems that Jammers were in two minds about where the axe of budget cuts should fall in Europe. But presuming that new structures will require new budgets, at the expense of others, policymakers will need to balance this love of the new with some tough assessments of the old.

## The enemy gets a vote, too

Jammers were often remarkably incisive and technically well informed when diagnosing some of the failures of the last decade's defence, security and military policy. From counter-insurgency in Afghanistan to counter-terrorism in Europe, the Jam featured a number of lessons-learned moments about how NATO and the EU could do better in tackling security threats.

However, as many Jammers also noted, the enemy gets a vote, too. As 19th Century strategist Helmuth von Moltke put it, 'no plan survives contact with the enemy', and the ability for foes to react and adapt in opposition to new security policies is well known.

As such, a great deal of emphasis was placed on the need to constantly review and improve in the face of enemy adaptation. New weaknesses will always be found by cunning opponents, and defence and security policy is thus a reactive process.

## It's the economy, stupid

Finally, the financial crisis, and its overbearing imperative to cut government spending across Europe, under-pinned the entire Jam discussion.

In fact, the actual topic of the current economic climate was barely directly discussed by Jammers; it was instead the status quo; as an understood existing factor that informed every aspect of the debate.

Hence, Jammers were at all times focused on streamlining existing processes, increasing cost efficiencies, finding the political will to invest and acknowledging the imperatives of both job creation and economic growth that must under-write all political discussion today.

Such tasks are not easy. But the universal appreciation of their importance demonstrates that even when speculating far into the future, Jammers were, in the end, rooted firmly in the realities of the present.

This combination made the debate stimulating and insightful.

# VI. Live chats

The 2012 Security Jam live chats were real-time discussions dedicated to a particular topic, hosted by think tank or NGO expets.

## 'Crisis, Information and Social Media'

Hosted by
**International Security Information Service, Europe (ISIS)**

Moderator:
**Philip Worré**
Executive Director

On March 19th 2012, ISIS Europe hosted a live chat on 'Crisis information and social media', in the framework of the 2012 Security Jam. During the 45 minute-long live conversation, participants discussed the rising importance of social media, their active or passive role in times of crisis, and the accuracy of the information they provide to their public. Paulo Brito, independent consultant in security and defence policy, exposed his point of view; that mainstream media remains more influential than social media. He saw a major contradiction in social media as it constitutes a useful tool to mobilize people, but at the same time, it does not manage to reach and connect to hard political power. Finally, he raised the problem of information flows possibly being tampered with external actors. The Kony 2012 'story' was at the core of the debate. Most participants, although critical of the Kony 2012 campaign, agreed that there was a differentiated impact of the video depending on the status and occupation of the audience, and that it had undoubtedly raised general awareness on the prevailing situation in Uganda. Thus, they admitted that social media had a mobilising power that was unheard of in the sphere of traditional channels. The crackdown on social bloggers in countries like China was mentioned as another manifestation of the 'blogosphere's' power as an instrument to shortcut political control and advocate for change. Participants underlined the inherent shortcomings of social media, as it privileges short, quick, easy, real-time information over in-depth, contextualized, accurate information. The criteria upon which mass scale filtering and analysis of information shared by social media could be based on, have been discussed several times. Some participants noted that the accountability of non-official sources was to be questioned, as social media could be as biased as official sources. The buzzword of the chat was: 'be your own filter, build your own network of people you know and trust'. The chat ended with participants agreeing that social media is important but it should be looked upon with great responsibility and should not be used as a single information source.


## 'Analysing impact for EU Member States – creating better buy-in for SSR missions'

Hosted by
**Geneva Centre for Democratic Control of Armed Forces (DCAF)**

Moderator:
**Giji Gya**
Head of the Deputy Director Office

There were a large number of participants contributing to a very lively debate highlighting important aspects of EU SSR missions and bringing up interesting suggestions on how to create better buy-in for member states.

A first emerging idea was the establishment of an EU SSR body in order for the EU to have a strong policy focus and an anchor for SSR planning. It was suggested that such a body would liaise closely with one single Ministry in each Member State and would be given the capability to pull political, development, security and resource reins of the EU, helping to diminish the CSDP/Commission divide. However, participants highlighted that the establishment of such a structure is not enough and needs to be accompanied by progress in substance, doctrine and effective lessons learned: there is currently no systematic framework or commonly agreed standards for evaluating all CSDP missions – although there is a lessons identified database for military missions and a lessons learnt database has just been developed for civilian missions. Still, however, identification and implementation of lessons learned and best practices happen ad hoc and are often based on inter-service agreements, using different approaches for different reports. At the same time, the EU needs to come up with better crisis analysis in order to gather necessary information regarding which is the appropriate instrument to deploy and when to transition.

On the CSDP/Commission divide, participants agreed that there needs to be a mechanism for better cooperation between the two bodies for joint exploitation of their capacities, taking advantage of the strengths and capacities of both, rather than seeking exclusivity.

Jammers further agreed that there is a current lack of formal and informal communication on SSR within the EU, but also externally. For example, although EU databases for both civilian and military lessons learned and best practice are in place, it is only known to a few stakeholders and has limited access. Production, demonstration and publication of the benefits, results and best practices of SSR would help enhance buy-in, where accountability and responsibility play an important role. As one participant noted, 'the process of communication is a confidence builder in itself and very much contributes to buy-in'.

cyber-security

forum

# energy

## Rape as a weapon of war: Raising awareness and finding tools to combat sexual violence in conflict

Academics, NGOs, policymakers and interested parties debated the issue of rape as a weapon of war in this 45 minute live online chat session hosted by WIIS Brussels. Participants to the chat session agreed that sexual violence in conflicts is a key issue for all women and men in the world. According to some, being a woman is the most dangerous position one can have in an armed conflict, even more than being a soldier. And while achievements have been made, more has to be done to raise the awareness of this fundamental attack on human rights.

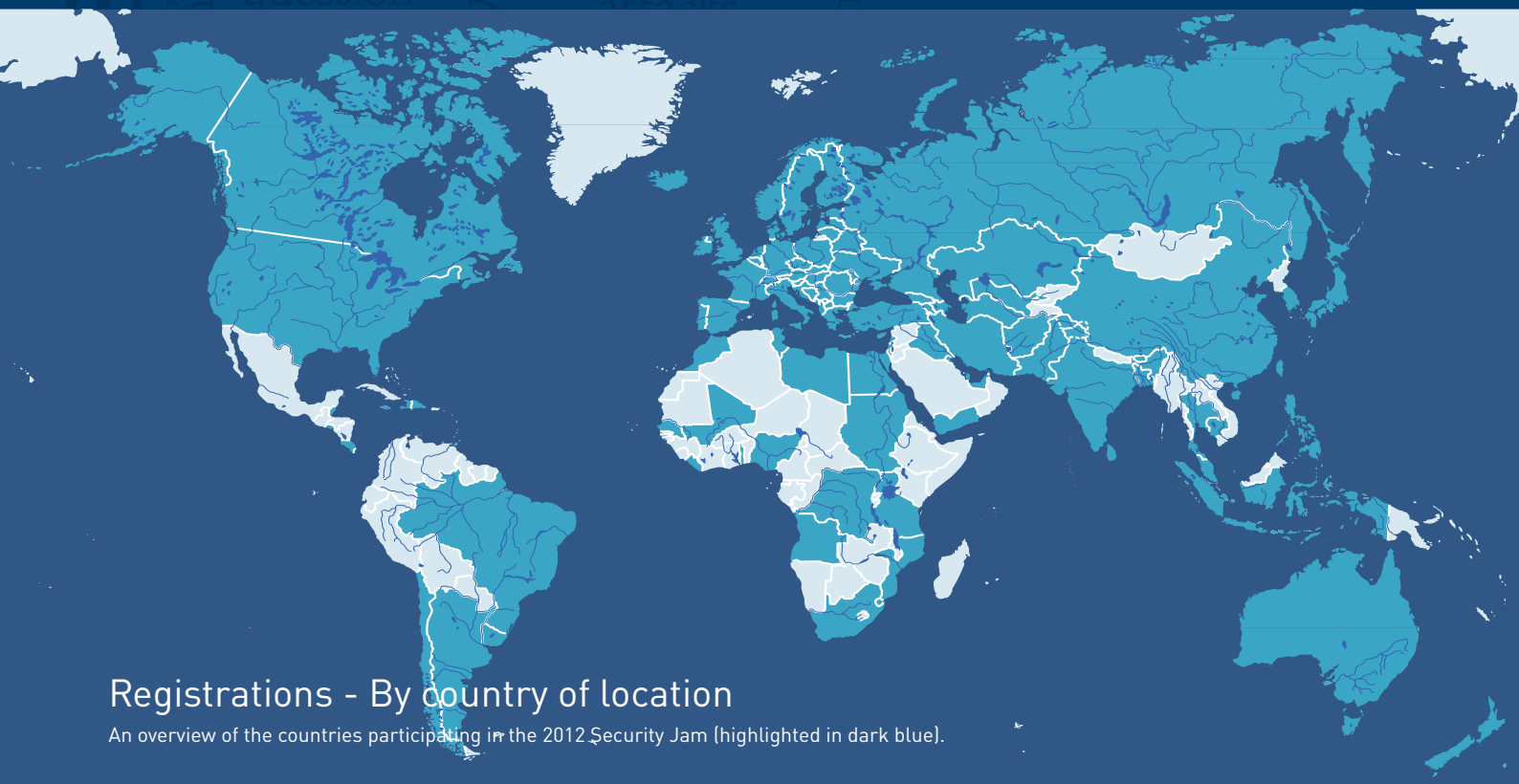
Several contentious issues were debated in the chat, including conditionality of development aid, the inclusion of provisions in peace negotiations and agreements, and how to solve the issue of sexual violence in conflict whilst not being seen as 'imposing Western values'. While not everyone agreed on means and measures, some proposed solutions included more resources for development of judiciary and penitentiary structures, targeting both male and female victims in outreach campaigns, and raising the issue with high level international policymakers.

In WIIS Brussels' concluding remarks, it was noted that addressing the question of impunity is fundamental, and that weak or non-existent Rule of Law structures should be reinforced either in conflict or post-conflict operations. Speaking from a Brussels perspective, EU policies do have the potential to influence or change situations if they are made a political priority. An EU Special Representative for Human Rights, with specific and clear responsibilities on gender issues could make a crucial impact in raising awareness and developing efficient policies. As such, a concrete conclusion and policy recommendation arose from the discussion is to encourage the EU to promptly make such a senior appointment.

Hosted by
**Women in International Security (WIIS)**
Brussels

Moderator:
**Cristina Gallach**
Head of Communication, Directorate-General for Press, Communication & Transparency, Council of the European Union

# VII. Statistics

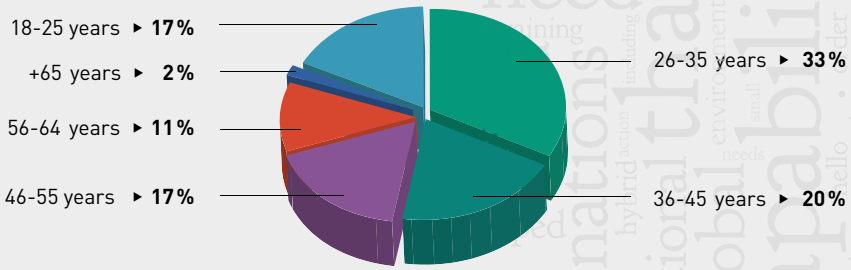


## Registrations - By country of location

An overview of the countries participating in the 2012 Security Jam (highlighted in dark blue).

## Age

### Age distribution of the Security Jam participants

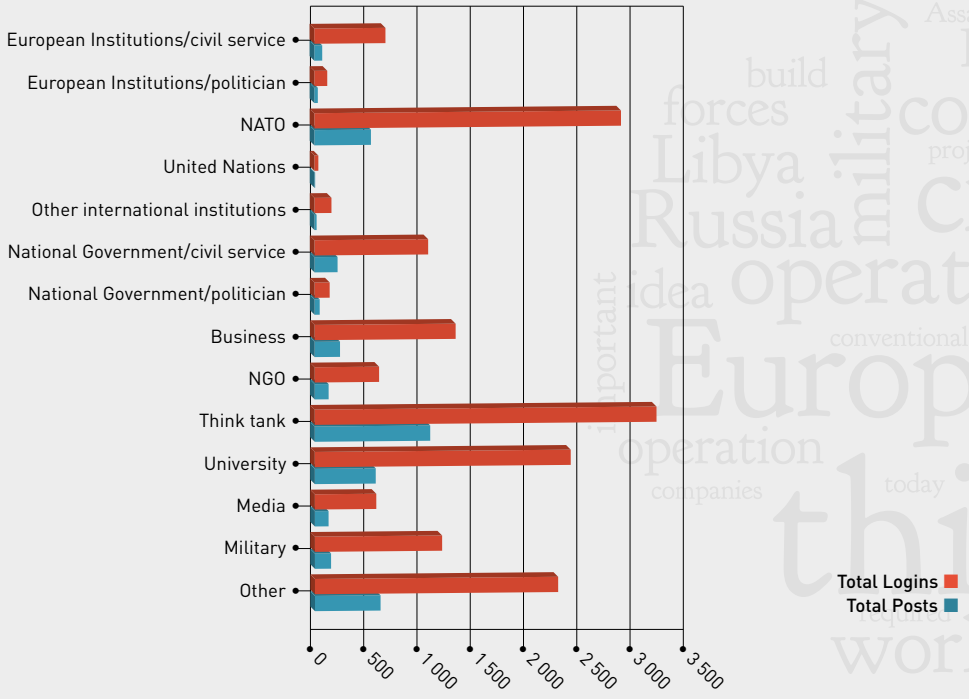



### Age distribution by forum

| Age range | Future Capabilities and Technologies | Int'l. cooperation in capabilities | Strategic Partnerships | Crisis Management | Facing the Cyber-Challenge | Transnational and Hybrid Threats | Object-lesson: Libya | Object-lesson: Afghanistan |
|---|---|---|---|---|---|---|---|---|
| 18-25 years | 128 | 113 | 45 | 70 | 73 | 84 | 101 | 53 |
| 26-35 years | 182 | 138 | 241 | 151 | 196 | 100 | 111 | 160 |
| 36-45 years | 131 | 91 | 121 | 139 | 131 | 55 | 30 | 65 |
| 46-55 years | 115 | 101 | 89 | 56 | 97 | 93 | 61 | 58 |
| 56-64 years | 47 | 55 | 64 | 68 | 71 | 48 | 49 | 25 |
| +65 years | 5 | 16 | 11 | 10 | 10 | 4 | 2 | 0 |

# Affiliation

## Relation between logins and posts by affiliation

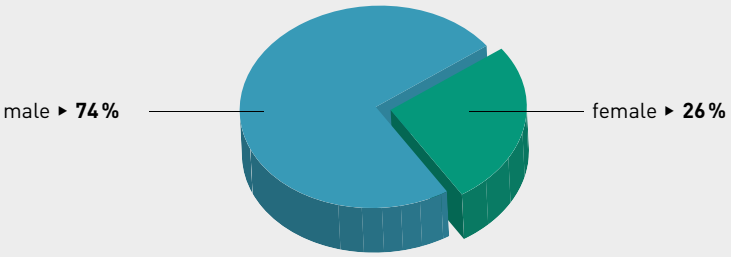



## Participation in the 8 forums differentiated by affiliation

| Affiliation | Future Capabilities and Technologies | Int'l. cooperation in capabilities | Strategic Partnerships | Crisis Management | Facing the Cyber-Challenge | Transnational and Hybrid Threats | Object-lesson: Libya | Object-lesson: Afghanistan |
|---|---|---|---|---|---|---|---|---|
| European Institutions/civil service | 3 | 8 | 23 | 18 | 9 | 1 | 10 | 3 |
| European Institutions/politician | 2 | 7 | 5 | 2 | 7 | 0 | 9 | 1 |
| NATO | 143 | 89 | 39 | 45 | 69 | 50 | 54 | 44 |
| United Nations | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 1 |
| Other international institutions | 1 | 3 | 5 | 2 | 2 | 0 | 2 | 5 |
| National Government/civil service | 14 | 23 | 42 | 40 | 62 | 18 | 1 | 17 |
| National Government/politician | 0 | 4 | 14 | 2 | 25 | 0 | 3 | 0 |
| Business | 71 | 48 | 21 | 25 | 39 | 21 | 10 | 4 |
| NGO | 16 | 15 | 26 | 27 | 18 | 12 | 6 | 11 |
| Think tank | 224 | 140 | 191 | 109 | 168 | 51 | 153 | 52 |
| University | 59 | 82 | 78 | 78 | 100 | 67 | 59 | 51 |
| Media | 8 | 11 | 25 | 19 | 17 | 24 | 13 | 12 |
| Military | 21 | 27 | 8 | 25 | 16 | 29 | 11 | 15 |
| Other | 46 | 57 | 94 | 99 | 46 | 111 | 20 | 145 |

# Gender

## Gender distribution of the Security Jam participants



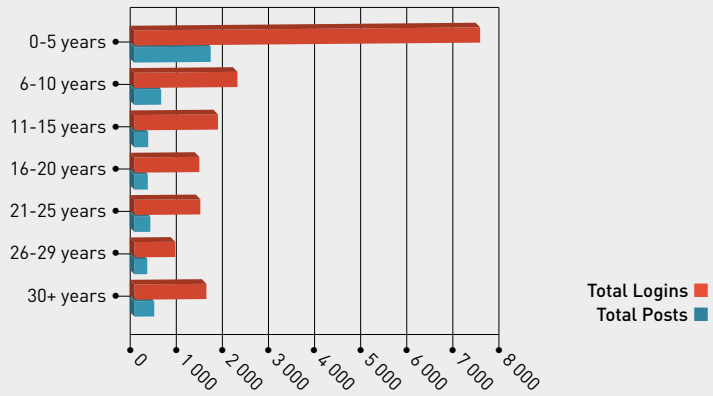

## Gender distribution by forum

| Gender | Future Capabilities and Technologies | Int'l cooperation in capabilities | Strategic Partnerships | Crisis Management | Facing the Cyber-Challenge | Transnational and Hybrid Threats | Object-lesson: Libya | Object-lesson: Afghanistan |
|---|---|---|---|---|---|---|---|---|
| Male | 477 | 375 | 416 | 367 | 465 | 264 | 242 | 244 |
| Female | 131 | 139 | 155 | 127 | 113 | 120 | 112 | 117 |

## Description: Post distribution by discussion forum

| | |
|---|---|
| Future Capabilities and Technologies | 608 |
| Facing the Cyber-Challenge | 578 |
| Strategic Partnerships | 572 |
| Int'l Cooperation in Capabilities | 514 |
| Crisis Management | 494 |
| Transnational and Hybrid Threats | 384 |
| Object-lesson: Afghanistan | 361 |
| Object-lesson: Libya | 354 |

## Years of experience in security, defence or development issues




### Participation in the 8 forums by years of experience

| Years of experience in security, defence or development issues | Future Capabilities and Technologies | Int'l cooperation in capabilities | Strategic Partnerships | Crisis Management | Facing the Cyber-Challenge | Transnational and Hybrid Threats | Object-lesson: Libya | Object-lesson: Afghanistan |
|---|---|---|---|---|---|---|---|---|
| 0-5 years | 271 | 233 | 234 | 227 | 203 | 169 | 172 | 139 |
| 6-10 years | 68 | 35 | 152 | 51 | 114 | 39 | 43 | 78 |
| 11-15 years | 28 | 47 | 39 | 29 | 46 | 17 | 33 | 60 |
| 16-20 years | 75 | 42 | 48 | 59 | 17 | 18 | 19 | 13 |
| 21-25 years | 31 | 34 | 24 | 28 | 133 | 70 | 4 | 20 |
| 26-29 years | 65 | 45 | 15 | 50 | 22 | 31 | 22 | 26 |
| 30+ years | 70 | 78 | 59 | 50 | 43 | 40 | 61 | 25 |

# VIII. VIP Jammers

**Claude-France Arnould**
Chief Executive, European Defence Agency

**Gen. Stéphane Abrial**
Supreme Allied Commander Transformation, NATO

**Giorgi Baramidze**
Vice Prime-Minister, Georgia

**Maj. Gen. Mark A. Barrett**
Deputy Chief of Staff, Strategic Plans and Policy, NATO Allied Command Transformation

**Gen. Knud Bartels**
Chairman, NATO Military Committee

**Isaac Ben-Israel**
Senior Cyber-Security Advisor to the Prime Minister, Israel

**Lt. Gen. Jürgen Bornemann**
Director General, International Military Staff, NATO

**Maj. Gen. Jochen Both**
Commander, European Air Transport Command

**Franziska Katharina Brantner**
Member of the Committee on Foreign Affairs, European Parliament

**Amb. Lawrence Butler**
Civilian Deputy to the Commander and Foreign Policy Advisor, United States European Command

**Barbara Contini**
Member of the Committee on Defence, Italian Senate

**Tarja Cronberg**
Member of the Committee on Foreign Affairs, European Parliament

**Brig. Gen. Giovanni Fungo**
Assistant Chief of Staff Capability Engineering, NATO Allied Command Transformation

**Ana Gomes**
Member of the Committee on Foreign Affairs, European Parliament

**Kolinda Grabar-Kitarovic**
Assistant Secretary General for Public Diplomacy, NATO

**Csaba Hende**
Minister of Defence, Hungary

**VAdm. Antonio Hernández**
Assistant Chief of Staff Joint Deployment and Sustainment, NATO Allied Command Transformation

**Ernest J. Herold III**
Deputy Assistant Secretary General for Defence Investment, NATO

**Lt. Gen. Kurt Herrmann**
Director CIS Services Agency, NATO

**David Heyman**
Assistant Secretary for Policy, United States Department of Homeland Security

**Brig. Gen. Roy Hunstok**
Director, Deployable Forces Integrated Project Team, NATO Allied Command Transformation

**VAdm. Anthony Johnstone-Burt**
Chief of Staff, NATO Allied Command Transformation

**Col. Hans-Jürgen Kasselmann**
Director, Civil-Military Cooperation Centre of Excellence

**Maj. Gen. Jon Berge Lilland**
Assistant Chief of Staff for Programme and Planning Management, NATO Allied Command Transformation

**Krzysztof Lisek**
Vice Chairman of the Subcommittee on Security and Defence, European Parliament


**Agostino Miozzo**
Managing Director for Crisis Response and Operational Coordination, European External Action Service

**Nickolay Mladenov**
Minister of Foreign Affairs, Bulgaria

**Zsolt Németh**
Minister of State for Foreign Affairs, Hungary

**Norica Nicolai**
Vice Chairwoman of the Subcommittee on Security and Defence, European Parliament

**Patrick Pailloux**
Director General, Agence Nationale de la Sécurité des Systèmes d'Information, France

**Ioan Mircea Paşcu**
Vice Chairman of the Committee on Foreign Affairs, European Parliament

**Maciej Popowski**
Deputy Secretary General, European External Action Service

**VAdm. Carol M. Pottenger**
Deputy Chief of Staff Capability Development, NATO Allied Command Transformation

**Jaan Priisalu**
Director General, Estonian Information Systems Authority

**Michael C. Ryan**
Deputy Director, Policy, Strategy, Partnership and Capabilities at the United States European Command

**Brig. Gen. Mark D. Scraba**
Director, Joint Interagency Counter Trafficking Center, United States European Command

**Jamie Shea**
Deputy Assistant Secretary General for Emerging Security Challenges, NATO

**Brig. Gen. Peter Sonneby**
Commander, Joint Analysis and Lessons Learned Centre, NATO

**Adm. James Stavridis**
Supreme Allied Commander Europe, NATO

**Vygaudas Usackas**
European Union Special Representative to Afghanistan, Delegation of the European Union to Afghanistan

**Lt. Gen. Ton van Osch**
Director General, European Union Military Staff, European External Action Service

**Alexander Vershbow**
Deputy Secretary General, NATO

**Col. Toine Visser**
Director, Command and Control Centre of Excellence, NATO

**Rob Wainwright**
Director, Europol

**Maj. Gen. Jaap Willemse**
Assistant Chief of Staff, Computers Intelligence Surveillance, Reconnaissance & Network Enabled Capabilities, NATO

**Catherine Woollard**
Executive Director, European Peacebuilding Liaison Office

# IX. Hosts

Our thanks go to the hosts and their organisations for their crucial role during the Security Jam 2012. Their work as moderators ensured high quality of debate and discussion that made the Jam an overwhelming success.

**Ian Anthony**
Director, Arms Control and Non-proliferation Programme, Stockholm International Peace Research Institute (SIPRI)

**Jorge Benitez**
Director of NATOSource, Atlantic Council of the United States

**Dave Clemente**
Research Assistant, International Security Programme, Chatham House

**Dustin Dehez**
Member of the Young Foreign Policy Experts, Konrad Adenauer Stiftung

**Hans de Vreij**
Independent Journalist

**Marcel Dickow**
Research Associate, Stiftung Wissenschaft und Politik (SWP)

**Bates Gill**
Director, Stockholm International Peace Research Institute (SIPRI)

**Camille Grand**
Director, Fondation pour la Recherche Stratégique

**Philippe Gros**
Research Fellow, Fondation pour la Recherche Stratégique

**Jeffrey Lightfoot**
Deputy Director of the International Security Program, Atlantic Council of the United States

**Lucia Marta**
Research Fellow, Fondation pour la Recherche Stratégique

**Robin Niblett**
Director, Chatham House

**Agnieszka Nimark**
Associate Researcher, Centro de Estudios y Documentación Internacionales de Barcelona (CIDOB)

**Daniel Nord**
Deputy Director, Stockholm International Peace Research Institute (SIPRI)

**Magnus Nordenman**
Deputy Director of the International Security Program, Atlantic Council of the United States

**Marco Overhaus**
Research Associate, Stiftung Wissenschaft und Politik (SWP)

**Joris van Esch**
Strategic Analyst, The Hague Centre for Strategic Studies (HCSS)

**Jordi Vaquer i Fanes**
Director, Centro de Estudios y Documentación Internacionales de Barcelona (CIDOB)

**Julian Voje**
Political scientist, Konrad Adenauer Stiftung

**Nicolai von Ondarza**
Research Associate, Stiftung Wissenschaft und Politik (SWP)

**Claire Yorke**
Programme Manager, Chatham House

**Peter Wijninga**
Strategic Analyst, The Hague Centre for Strategic Studies (HCSS)


# Facilitators

Our thanks go to all the facilitators for their precious help in monitoring the discussions and supporting moderation during the Security Jam 2012.

**Tessa Ax**
The Netherlands

**Riley Barnes**
United States of America

**Deacon Benedict**
Germany

**Cathleen Berger**
Germany

**Robert Blaszczak**
United Kingdom

**Erik Brattberg**
United States of America

**Carles Castello-Catchot**
United States of America

**Nicolas De Pedro**
Spain

**Agnieszka Dudziak**
Germany

**Eleni Ekmektsioglou**
Greece

**Igor Garcia-Tapia**
Spain

**Juan Garrigues**
Spain

**Lina Grip**
Sweden

**Sarma Hriday**
India

**Demetrios Klitou**
Cyprus

**Simona Kordosova**
United States of America

**Elaine Korzak**
United Kingdom

**Marc Larance**
France

**Maxime Larivé**
France

**Hannah Ledger**
United Kingdom

**Markus Mayr**
Germany

**Stephen Mintz**
United States of America

**Martha Molfetas**
United States of America

**Valentina Morselli**
Belgium

**Hanna Nõmm**
United Kingdom

**Elias B. Okwara**
Kenya

**Kyle Pfeiffer**
United States of America

**Andrew L. Porter**
Germany

**Sameer Punyani**
United States of America

**Ioana-Maria Puscas**
Belgium

**Sophie Roborgh**
The Netherlands

**Hina Sarfaraz**
Pakistan

**Yana Staykova**
France

**Catherine Stella Schmidt**
United States of America

**Elsa Testelin**
The Netherlands

**Magdalena Tsankova**
Bulgaria

**Evert Faber van der Meulen**
The Netherlands

**Renata Zaleska**
Belgium

**Grace Zec**
The Netherlands

**Ioanna Nikoletta Zyga**
Greece

**Liu Yanchuan**
China

# Further recommendations

**The 2012 Security Jam – other recommendations you might have missed...**

- NATO should endorse a 'hybrid threats' concept to better plan for and deal with non-state actors and terrorist groups.
- The EU should form a permanent security sector reform department.
- NATO member navies should cooperate on the construction of a common frigate and littoral class warship, with interoperable maritime surveillance and drone networking systems.
- The US should join Canada and other Northern European Allies in formulating a NATO Arctic Security policy.
- The EU and NATO should coordinate a reserve forces policy, aimed at increasing the number of reservists which could be deployed for non-combat crisis management roles.
- NATO security engagement with Afghanistan post-2014 should expand to include the Shanghai Cooperation Organisation and Pakistan more formally.
- The EU should directly subsidize nations which pool & share military equipment using the Union's Structural Funds.
- NATO must prioritize and invest in situational awareness and object tracking systems for the space domain.
- India should be approached as a more permanent security and defence partner by NATO.
- Electro-Magnetic Pulse (EMP) damage and related technology should be classed as a potential cyber-threat.
- EU Foreign Affairs Ministerial meetings should be preceded by an online 'information conference' on the countries under discussion.
- The international shipping community should upload camera and sensor feeds into a 'wiki' maritime surveillance hub for open-source data.
- 'Geo-weaponeering' – the exploitation of natural disasters by a follow up unconventional or cyber-based terrorist attack – should be addressed in crisis response planning.
- European nations should fund a large scale cyber-security public awareness campaign.

**SECURITY & DEFENCE AGENDA**
Bibliothèque Solvay
137 rue Belliard
1040 Brussels
Tel: +32 (0)2 737.91.48
Fax: +32 (0)2 736.32.16
Email: info@securitydefenceagenda.org
Web: www.securitydefenceagenda.org


Coalition partners:

Media partners: