ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Tom Parkhouse
Leendert van Bochoven

An Agenda for NATO-EU-Private Sector Cyber Collaboration

While there has been much talk of cyber security cooperation between NATO and the European Union, there has been little action. Likewise, while NATO and the EU both collaborate with the private sector, it has been is ad hoc and failed to seize strategic opportunities.

The internet has done so much to break down barriers of geography and jurisdiction, creating opportunity and new risks, but we have yet to see a corresponding revolution in the relationship between government, corporate, and transnational approaches to cyber security.

This issue brief discusses the roles and rationale for NATO, the EU, and the private sector to work together on cyber issues; highlights six key areas that should be the focus of action; and addresses the challenges to cooperation.

EU and NATO Cyber Roles

While the aim of both NATO and EU was originally to reduce the likelihood of war in Europe, the means by which they set about to achieve this were very different. NATO is a political-military alliance that serves as the ultimate guarantor of the security of the transatlantic space. As such, it needs to be able to deter and respond to the most serious cyber attacks with the appropriate response from all the means available to it. The EU is a parliamentary, economic, and trading institution that has the necessary powers to legislate and enforce uniform cyber security standards for its twenty-seven member states.

There have been many calls for increased cooperation between NATO and the EU, and between both organizations and the private sector. Alas, while there is considerable

The Smarter Alliance Initiative

This issue brief is part of the Smarter Alliance Initiative, a partnership between the Atlantic Council and IBM, established in response to Secretary General Anders Fogh Rasmussen's call for NATO members to adopt a "smart defense" approach to leveraging scarce resources to develop and sustain capabilities necessary to meet current and future security challenges in an age of austerity.

Working with recognized experts and former senior officials from Europe and the United States, the Atlantic Council and IBM have produced a set of policy-oriented briefs focused on NATO reform and cyber security, with the aim to provide thought leadership and innovative policy-relevant solutions for NATO's continued organizational reform and role in cyber security.

The publications and their findings will be showcased at public and private events for the defense policy and NATO communities on both sides of the Atlantic.

For more information about the Smarter Alliance Initiative, please contact Barry Pavel, Director of the Atlantic Council's Brent Scowcroft Center on International Security, at **bpavel@acus.org** or Leendert van Bochoven, NATO and European Defense Leader, IBM, at **L_van_Bochoven@nl.ibm.com**.

Tom Parkhouse is an Atlantic Council nonresident senior fellow and a former Royal Air Force officer working on cyber issues.

Leendert van Bochoven is NATO and European Defense Leader for IBM.

overlap in the membership of NATO and the EU, there is very little consensus on exactly what shape cyber cooperation should take. The EU has a plethora of cyber initiatives promoted by its various institutions and Commissioners which tend to fall into two categories: those that seek to develop the economic and social opportunities afforded by the availability of internet-based services, and those that seek to improve critical infrastructure protection as a security issue. There is scant mention of the need for cooperation with NATO in any of these documents.

Conversely, while NATO's foray into cyber is more recent and less developed, all the emerging frameworks underscore a need for EU involvement. NATO's New Strategic Concept, agreed to in Lisbon in November 2010, noted the necessity of improving the Alliance's ability to prevent, detect, defend against, and recover from cyber-attacks; and the subsequent announcement of the NATO Cyber Policy emphasized the need for cooperation with the EU.

Likewise, in a May 2011 report, Lord Jopling, the General Rapporteur to the NATO Parliamentary Assembly Committee on the Civil Dimension of Security, recognized not only the importance of closer cooperation with the EU because of its ability to deliver legislation on cyber issues, but also with the private sector as custodians of many critical national infrastructures and specifically IT companies who develop the hardware and software used by most internet users.

The United Kingdom House of Lords' European Union Committee in their report on *Protecting Europe Against Large-Scale Cyber-Attacks* also recognized the considerable cyber defense overlap between the roles of the EU and NATO. This body called on both organizations to develop urgently a coherent approach to working together and further suggested that NATO-EU cyber cooperation should be formally codified.

The Private Sector

Both the EU and NATO have stated clearly that they recognize the importance of the private sector—both for the internet backbone as well as the management of most of the private networks and infrastructure relied upon by the organizations and their member nations.

NATO-EU cooperation remains mostly transactional and fails to integrate the respective strategic strengths of these powerful organizations.

It comes as a surprise to many officials that the private sector has a vast amount of data about the internet traffic that passes over its systems and is able to develop outstanding intelligence about the capabilities and activities of users—intelligence is often as good as that in many governments, but can be more easily shared. Executives representing IT corporations often publicly comment that they would welcome improved cooperation with governmental institutions[1,2]. They are bemused that state institutions often work so hard to generate information that could be made available to them at low cost and enhanced with their cooperation.

To help tap into this information, Neelie Kroes, the vice president of the European Commission responsible for the EU Digital Agenda, has advocated improved public-private partnership with particular focus on information sharing and response to cyber attacks. Her vision is that the private sector should be incentivized to improve cyber security and that public money should be used to supplement private sector cyber security research, thus spreading the burden of innovation. It remains to be seen if these proposals can survive the drafting process and be enshrined in the European Strategy for Internet Security due to be released later this year.

Challenges of Cyber Cooperation

Not everyone believes that there is clear evidence of a serious cyber threat; some suggest that loud voices in the defense, security, and intelligence communities are seeking to perpetuate their own importance and income streams. Without persuasive accessible information for the public and elected representatives, they will remain skeptical until impacted themselves.

At the 2011 Munich Security Conference, Herman Van Rompuy, the president of the European Council, declared that cyber is an issue that effects all the nations in the

1 David Rockvam, Entrust at **http://www.infosecurity-magazine.com/view/27282/comment-cybersecurity-and-information-sharing-is-a-twoway-street/**

2 John Linkous, CEO of eIQnetworks at **http://www.cso.com.au/article/424545/public_vs_private_cyberattack_responsibility_debate_heats_up/**

Euro-Atlantic security community and proposed that the partnership between NATO allies and EU member states to address shared cyber issues should be based on practical cooperation and not discriminate against any participating state. Yet, as in any political institution, the Domestic politics of member nations, most notably the perpetual dispute between Greece and Turkey, can also threaten cooperation between the EU and the Alliance. More broadly, public distrust of Brussels-based bureaucracies frustrates shared agendas. Just as NATO is seen by some as a right-wing bastion of the defense-industrial establishment, others perceive the EU as threatening national sovereignty and slow to deliver harmonization.

For many, any program that appears to expand the remit of either institution will not be acceptable during a period of austerity. This view must be countered with arguments persuading policymakers and citizens alike that in a globalized world, a secure cyber environment will encourage investment in the Euro-Atlantic area, increase competitiveness of Euro-Atlantic business, and promote export of Euro-Atlantic cyber security products. The costs of protecting Euro-Atlantic security must be shown to be a necessary expense that delivers a credible outcome of value to the whole community.

Six Items for the Collaboration Agenda

The leadership of the Euro-Atlantic community must act together and in concert with industry to address the issues of this digital age, to safeguard a treasured way of life, and to enable the exploitation of opportunities.

The agenda proposed below aims to deliver tangible evidence of cooperation between NATO, the EU and the private sector. The successful execution of the agenda should reduce skepticism about the threats emanating through cyberspace, focus scarce resources on key activities that will foster confidence, and reduce the risk of political confusion either exacerbating a conflict situation or falling to address a growing threat.

Agenda Item: Improve EU-NATO and Industry Coordination

NATO and EU decision makers need to be able to detect attacks against their institutions and member states, to correctly identify the attack and its origin (using all source intelligence). Given that the critical infrastructure of North America and Europe is generally managed by the private sector, that any attack will have traversed the privately-owned internet backbone, and that the payload will have been delivered by the contracted internet service provider, it is inconceivable to think that government can detect malicious cyber activity without cooperation from the private sector.

The proposed Computer Emergency Response Team for the EU (CERT-EU) must have clear and direct linkages with the NATO Computer Incident Response Centre (NCIRC) as well as with nation state CERTS which, under the EU Digital Agenda, EU members are under remit to establish by the end of this year. NATO CIRC should also become a member of the European Government CERT Group.

The CERT-EU as well as NCIRC should become public-private partnerships with security-cleared industry representatives co-located with them able to provide access to the vast swathes of data they hold. The process of information sharing should be two-way and as levels of trust increase the tipping and cueing effect should grow; there will be issues of competition and intelligence law that need to be worked through and political intervention may be necessary in order to achieve the opportunity offered.

Agenda for Collaboration

1. Improve EU-NATO and Industry Coordination
2. Blend Private Sector and Government Intelligence
3. Establish EU-NATO Protocol for the Investigation of Attacks on National Security Assets
4. Agree EU-NATO Protocol on Cyber Incident Response and Escalation
5. Coordination of NATO and EU Cyber Best Practice and Outreach
6. NATO and EU Leaders to Demonstrate Coherence on Security in a Digital Age

Both CERT-EU and the NATO CIRC should have senior IT industry representatives on their steering groups to oversee the process of integration and to ensure that tough issues are tackled by senior stakeholders.

Agenda Item: Blend Private Sector and Government Intelligence

What private sector malware detection services generally lack is the intelligence about cyber attacks derived from human resources-, imagery-, measurement and signature-, and signals intelligence available only to sophisticated nation states. Nation states, the EU, and NATO need initiatives that can blend the cyber intelligence available from private sector companies and the all source intelligence available from governments so that each can be used to cue the other.

Complicating this agenda is the fact that government generated intelligence generally attracts a security classification that prevents sharing. This flawed risk model either promotes duplication or limits the opportunity for fusing intelligence gained by different organizations, and prevents critical stakeholders from being briefed on the best constructed intelligence picture. While the source of intelligence and the means of gathering it need to be protected, the underlying information must be made available at more usable classifications.

As the EU External Action Service begins to enhance its operations, the question of how nation states, NATO, and the EU cooperate on intelligence issues is upon us anyway; the need for improved cyber-intelligence raises the stakes.

Agenda Item: Establish EU-NATO Protocol for the Investigation of Attacks on National Security Assets

It should not be assumed that an attack on a national security asset is a state-sponsored attack; indeed the majority of attacks that any organization will suffer will be criminal in their nature and therefore the default route for investigation should be through law enforcement channels. While one-off attacks may be damaging, it is likely that well-planned long-term assaults on European confidence in the digital environment will be more insidious and destabilizing.

NATO is not a law enforcement organization, and it should not try to be one. Law enforcement is the responsibility of the EU and nation states. But there needs to be a method whereby cyber attacks can be traced and tracked so that campaigns that go beyond the limited remit of the law enforcement community can be escalated. Alongside EU institutions, NATO needs a direct relationship with EUROPOL's cyber crime centre to ensure that non-traditional assaults on European strategic assets can be quickly and confidently identified as attacks on critical infrastructures.

Agenda Item: Agree EU-NATO Protocol on Cyber Incident Response and Escalation

Cyber incidents need to be escalated to the level whereby the perpetrator can be brought to account, and the series of incidents curtailed. The means of achieving this may require the diplomatic efforts of nation states. Equally, now that the EU External Action Service has a foreign ministry and diplomatic corps, it can have a role to play in diplomatic actions. Ultimately, escalation may mean invoking consultation between Alliance members under the auspices of Article 4 of the North Atlantic Treaty for consultation and potentially even Article 5 for collective action.

Escalation can include the ability to threaten a more confrontational, painful, or otherwise "less comfortable" state of relations between the parties. While NATO can threaten potentially unlimited military action, and the EU can warn of direct economic consequences, there is an obvious need for a harmonized process of response to the most serious cyber attacks.

If a major cyber attack does unfold, government must conduct diplomatic actions and military while industry is engaged in remediation and recovery. Determining attribution – or the nation most responsible – will need to be swift which will also require cooperation between industry, nations, the EU and NATO.

Europe is yet to face an overwhelming cyber attack. Before it does, it should model and exercise the response and escalation process, testing it in a variety of scenarios including state-sponsored/supported acts and actions by criminal/terrorist organizations.

Of course, if NATO is to act as an ultimate guarantor of security from all threats, including cyber threats, then it must be capable of operating after a debilitating cyber attack on its own systems, and the critical infrastructure needed by the alliance to generate and sustain its forces. The first step to achieving and maintaining such a battle-winning capability is

for NATO and its members to understand the cyber dependencies it has—and this will require significant cooperation from industry and will invariably involve assets that are critical to the EU as well. Only once understanding is achieved can prioritization and mitigation be successful.

Agenda Item: Coordination of NATO and EU Cyber Best Practice and Outreach

In 2011, both the EU's European Network and Information Security Agency (ENISA) in Crete and NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia faced questions about their relevance to their Brussels headquartered sponsors. Both have received enhanced mandates to be bastions of best practices and to deliver outreach. Given that both organizations have limited capabilities but work with similar audiences, it may make sense to align their work programs.

ENISA has a Permanent Stakeholder Group that includes industry representatives; a similar model of industry involvement should be considered at the CCDCOE so as to synchronize research and engagement activities with industry efforts. It might also be sensible to include an EU/EEAS/ENISA representative on the CCDCOE oversight board and the NATO Cyber Defense Management Board to ensure alignment. Similarly, NATO should be represented in key EU cyber fora especially in those areas being overseen by the EEAS and both organizations should cooperate on cyber capacity building especially in Africa and the Middle East.

Agenda Item: NATO and EU Leaders to Demonstrate Coherence on Security in a Digital Age

Computer networking, social media, and mobile devices have changed the way connected citizens operate and see themselves in the world. Massive economic opportunity has been borne of the technological developments that have underpinned much of our globalized, just-in-time world. In addition, just as the positives have changed the way we do business with the reward of efficiency and effectiveness, the negatives aspects will demand changes too.

The digital revolution is influencing all aspects of government, commerce, and personal life. Cyber security is not a niche item that can be separated from the other aspects of government, business, or social engagement. The fact is that all aspects of our lives need to be updated to ensure that they are not vulnerable in the 21st Century. This means that all government departments—not just defense, intelligence and security agencies—need to be taking cyber security seriously. Similarly, cyber security is an agenda item for all leaders in society and commerce, not just IT managers and chief information officers.

But as a cross-cutting issue, cyber security does need champions, advocates, sherpas and czars. Europe needs its political and industrial leaders to speak coherently and mainstream discussion about cyber security issues. They should promote understanding of the fragility of our digital society and the need to harden our critical assets. The promised EU Strategy for Internet Security should be refocused to be a Strategy for Security in a Digital Age, and designed to be relevant to everyone not just those who see themselves as par of the net generation.

Conclusion

The Euro-Atlantic community is at risk of failing to deliver the collaborative structures necessary to exploit the opportunities and neutralize the risks of living and working in an ever increasing digital environment.

NATO, the EU, and the private sector must adopt an agenda that includes coordination of monitoring and detection capabilities, sharing intelligence, and linking investigation to response and escalation. This cooperation should be underpinned by agreement on a single set of standards, common best practice and coordinated outreach activity.

Effective leadership will be essential if these changes are to be delivered against a back-drop of skepticism about the threats in cyberspace, the ongoing financial turmoil and calls for austerity, and concern about enlarged institutions.

But the prize is worthwhile—a secure cyber environment will encourage investment in the Euro-Atlantic area, will increase the competitiveness of Euro-Atlantic business, and promote the export of Euro-Atlantic cyber security products. It will keep our populations safe and secure from the risks of working and living in the digital age.

OCTOBER 2012

Visit www.acus.org for other publications from the Cyber Statecraft Initiative:

- NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow (IBM Smarter Alliance Initiative series)
- Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO (IBM Smarter Alliance Initiative series)
- When "Not My Problem" Isn't Enough: Political Neutrality and National Responsibility in Cyber Conflict
- Preparing for Cyber 9/12
- The US Cyber Policy Reboot
- The Spectrum of National Responsibility for Cyberattacks
- The Five Futures of Cyber Conflict and Cooperation
- Beyond Attribution: A Vocabulary for National Responsibility for Cyberattacks
- Bringing a Gun to a Knife Fight: US Declaratory Policy and Striking Back in Cyber Conflict
- Pursuing Cyber Statecraft

The Atlantic Council's Board of Directors

CHAIRMAN
*Chuck Hagel

CHAIRMAN, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

VICE CHAIRS
*Robert J. Abernethy
*Richard Edelman
*C. Boyden Gray
*Richard L. Lawson
*Virginia A. Mulberger
*W. DeVier Pierson

TREASURER
*Brian C. McK. Henderson

SECRETARY
*Walter B. Slocombe

DIRECTORS
Odeh Aburdene
Timothy D. Adams
*Michael Ansari
Richard L. Armitage
Adrienne Arsht
*David D. Aufhauser
*Ziad Baba
Elizabeth F. Bagley
Ralph Bahna
Sheila Bair
Lisa B. Barry
*Thomas L. Blair
Julia Chang Bloch
Francis Bouchard
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
Daniel W. Christman
Wesley K. Clark
John Craddock
David W. Craig
Tom Craren
*Ralph D. Crosby, Jr.
Thomas M. Culligan
Gregory R. Dahlberg
Brian D. Dailey
*Paula J. Dobriansky
Christopher J. Dodd
Markus Dohle
Lacey Neuhaus Dorn
Conrado Dornier
Patrick J. Durkin
Thomas J. Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Dan-Åke Enstedt
Julie Finley
Lawrence P. Fisher, II
Alan H. Fleischmann
Michele Flournoy
*Ronald M. Freeman
*Robert S. Gelbard
Richard L. Gelfond
Edmund P. Giambastiani, Jr.
*Sherri W. Goodman
John A. Gordon
*Stephen J. Hadley
Mikael Hagström
Ian Hague
Frank Haun
Rita E. Hauser
Michael V. Hayden
Annette Heuser
Marten H.A. van Heuven
*Mary L. Howell
Robert E. Hunter
Robert L. Hutchings
Wolfgang Ischinger
Deborah James
Robert Jeffrey
*James L. Jones, Jr.
George A. Joulwan
Stephen R. Kappes
Francis J. Kelly, Jr.
Zalmay M. Khalilzad
Robert M. Kimmitt
Roger Kirk
Henry A. Kissinger
Franklin D. Kramer
Philip Lader
David Levy
Henrik Liljegren
*Jan M. Lodal
*George Lund
*John D. Macomber
Izzat Majeed
Wendy W. Makins
Mian Mansha
William E. Mayer
Eric D.K. Melby
Franklin C. Miller
*Judith A. Miller
*Alexander V. Mirtchev
Obie Moore
*George E. Moose
Georgette Mosbacher
Bruce Mosler
Hilda Ochoa-Brillembourg
Philip A. Odeen
Sean O'Keefe
Ahmet Oren
Ana Palacio
Torkel L. Patterson
*Thomas R. Pickering
*Andrew Prozes
Arnold L. Punaro
Kirk A. Radke
Joseph W. Ralston
Teresa M. Ressel
Jeffrey A. Rosen
Charles O. Rossotti
Stanley O. Roth
Michael L. Ryan
Harry Sachinis
William O. Schmieder
John P. Schmitz
Kiron K. Skinner
Anne-Marie Slaughter
Alan J. Spence
John M. Spratt, Jr.
Richard J.A. Steele
James B. Steinberg
Philip Stephenson
*Paula Stern
John Studzinski
William H. Taft, IV
John S. Tanner
Peter J. Tanous
*Ellen O. Tauscher
Clyde C. Tuggle
Paul Twomey
Henry G. Ulrich, III
Enzo Viscusi
Charles F. Wald
Jay Walker
Michael F. Walsh
Mark R. Warner
J. Robinson West
John C. Whitehead
David A. Wilson
Maciej Witucki
R. James Woolsey
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
Robert M. Gates
Michael G. Mullen
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
James R. Schlesinger
George P. Shultz
John W. Warner
William H. Webster

LIFETIME DIRECTORS
Carol C. Adelman
Lucy Wilson Benson
Daniel J. Callahan, III
Kenneth W. Dam
Stanley Ebner
Barbara Hackman Franklin
Chas W. Freeman
Carlton W. Fulford, Jr.
Geraldine S. Kunstadter
James P. McCarthy
Jack N. Merritt
Steven Muller
William Y. Smith
Marjorie Scardino
Helmut Sonnenfeldt
Ronald P. Verdicchio
Carl E. Vuono
Togo D. West, Jr.

**Executive Committee Members*
List as of September 17, 2012

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1101 15th Street, NW, Washington, DC 20005 (202) 463-7226
www.acus.org