ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Jason Healey
Leendert van Bochoven

SMARTER ALLIANCE INITIATIVE

NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow

NATO's central missions of collective defense and cooperative security must be as effective in cyberspace as they are in the other domains of air, land, sea, and space. The Alliance started this process after suffering its first major cyber attacks in 1999, during Operation Allied Force, but more than a decade later it is still playing catch up. The recent NATO cyber defense policy gives the Alliance a strong boost, giving priority to defense of NATO's own networks. But now the Alliance should "double down" on a core set of priorities, leveraging the best capabilities, policies, and practices from member nations and industry partners.

To make this case, the first section of this Issue Brief touches on NATO's cyber past: the experience the Alliance has earned from more than a decade of cyber incidents, and the policies and capabilities that have resulted. The paper then looks at NATO's present, the existing set of policies and organizations, and concludes with a discussion of NATO's future cyber capabilities. This last section examines major issues NATO will have to address, along with specific recommendations.

NATO's Cyber Past

Cyber defense has been part of NATO's agenda for more than a decade. In 2002 the Cyber Defense Program was adopted at the Prague Summit, at least partially in response to widely reported attacks on NATO organizations and Alliance nations carried out by activists from Serbia, Russia, and China during operation Allied

The Smarter Alliance Initiative

This issue brief is part of the Atlantic Council's Smarter Alliance Initiative in partnership with IBM. The Atlantic Council and IBM established the Smarter Alliance Initiative in response to the NATO Secretary General's call for NATO members to adopt a "smart defense" approach to leveraging scarce defense 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 in the run-up to the NATO Chicago Summit. The events will coincide with reform and policy development milestones established by the November 2010 NATO summit in Lisbon, Portugal.

For more information about the Smarter Alliance Initiative please contact:

Barry Pavel, Director of the Program on International Security, Atlantic Council, at **bpavel@acus.org**

Leendert van Bochoven, NATO and European Defense Leader, IBM, at **L_van_Bochoven@nl.ibm.com**

Jason Healey is director of the Atlantic Council's Cyber Statecraft Initiative. **Leendert van Bochoven** is leader for NATO and European defense at IBM.

Box 1: NATO's Cyber Past: Allied Force (1999)

A flurry of cyber incidents against NATO and member governments and militaries occurred during ALLIED FORCE in 1999 to force Serbian military units out of Kosovo. These incidents included denial of service attacks and defacements of the webpage for the Supreme Headquarters Allied Powers Europe while the US military saw a tripling of defacement attacks.

These protest attacks were conducted by nationalist Russian, Serbian, and Chinese hackers (after the accidental bombing of their embassy in Belgrade).

Force (see Box 1). The most important element of the Program was creation of the NATO Computer Incident Response Capability (NCIRC), the Alliance's "first responders" to prevent, detect, and respond to cyber incidents.

While NATO continued over the years to issue guidance—such as the Prague Capabilities Commitment of 2002 and the Comprehensive Political Guidance of 2005—it was not until the 2007 attacks against Estonia (see Box 2) that the Alliance truly realized the technical scale and political implications of potential cyber attacks. As a result, the 2008 Bucharest Summit emphasized "the need for NATO and nations to protect key information systems; to share best practices; and to provide a capability to assist Allied nations, upon request, to counter a cyber attack."

Out of the Bucharest Summit, the Alliance leadership established two major cyber defense institutions: the Cyber Defense Management Authority (CDMA) and the Cooperative Cyber Defense Center of Excellence (CCDCOE). The CDMA—under the governance of the Cyber Defense Management Board—became fully operational in April 2008 to initiate and coordinate cyber defenses, review capabilities and conduct appropriate security risk management. CDMA also helps member states to improve their own national cyber defense capabilities. The CCDCOE in Tallinn, Estonia does not have an operational cyber mission, but complements the work of the CDMA and NCIRC by improving cooperation and information sharing, such as through education and reviews of lessons learned. The Tallinn center has been particularly influential in legal issues by convening together practicing lawyers and legal academics from around the Alliance.

In response to demand for a capability to assist Allies seeking NATO support in protection or response, NATO is developing other options, such as Rapid Reaction Teams (RRTs). Scheduled to be fully operational by 2012, the RRTs will deploy security professionals to trouble spots when asked by the political leadership of a NATO nation threatened with or under attack. While the RRT will provide technical advice (helping to protect and restore systems or coordinating the response) its main value may be political, displaying unity to the people of the attacked Ally, within the Alliance and NATO headquarters, and to the leadership of nations sponsoring or conducting the attacks.

NATO's Strategic Concept and the 2010 Lisbon Summit Declaration continued a focus on defensive improvements. NATO leaders recognized the likely cyber dimension of future conflicts and committed to further improve capabilities to detect, assess, prevent, defend, and recover in case of a cyber attack. To this end, the Lisbon Capabilities Package addressed the most pressing gaps, including improvements to the NCIRC.

Box 2: NATO's Cyber Past: Estonia (2007)

In April and May of 2007, the relocation of a Soviet-era war memorial unleashed a series of large and sustained distributed denial-of-service attacks (DDoS attacks) flooding networks or websites with attack traffic so that it becomes inaccessible.

The attacks—many of which came from Russia, written in Russian, or coordinated on Russian websites—disabled the websites of the Estonian President, parliament and ministries along with websites of political parties, banks and news agencies. In phases of varying intensity, the attacks lasted for more than three weeks.

No evidence appears to directly link the attacks to the Russian government; however it was at least ignored and likely encouraged by Moscow.

Box 3: NATO's Cyber Present: Operation Unified Protector (2011)

Compared to Allied Force in 1999, during the operation to protect civilians in Libya, NATO cyber defenders had an easy time, with only three significant incidents:

1. Anonymous publicly warning NATO not to challenge it after a report on hactivism specifically mentioned the group; Anonymous then claimed to have intruded into a NATO server and extracted a large amount of data.

2. Hackers, probably associated with the hacker group Lulzsec, intruded into a single "NATO" website (actually an affiliated bookstore) and posted the names, usernames and passwords of the 12,000 registered users.

3. The Norwegian military reported suffering a malicious software attack one day after beginning NATO bombing operations in Libya.

None of these incidents had any significant impact, were directly tied to the operations, or and received much press. NATO's improved defenses since 1999 likely helped thwart more serious incidents.

NATO's Cyber Present

The Cyber Defense Policy and Action Plan of June 2011 are by far the most important steps the Alliance has taken so far to mature its cyber capabilities. Approved while NATO was conducting air operations over Libya (see Box 3), these aim to enhance the political and operational mechanism of NATO's response capability and expand training and assistance to improve defenses of Alliance national militaries. The main elements of the new approach include:

1. Realization that cyber defense is required to perform NATO's core tasks of collective defense and crisis management;

2. Prevention, resilience, and defense of cyber assets critical to NATO and its constituent Allies;

3. Implementation of robust cyber defense capabilities and centralized protection of NATO's own networks;

4. Definition of minimum requirements for cyber defense of national networks critical to NATO's core tasks;

5. Assistance to the Allies to achieve a minimum level of cyber defense to reduce vulnerabilities of national critical infrastructure; and

6. Engagement with partners, other international organizations, the private sector, and academia.

To implement these new policies and capabilities, the main NATO governance body for cyber defense, the Cyber Defense Management Board (the CDMB, which appears to have supplanted the CDMA), has been signing memoranda of understanding with the appropriate authority in each member nation. As of January 2012, nearly twenty such agreements have been signed. Progress will be reported "regularly" to the Alliance's highest political body, the North Atlantic Council.

In addition, the new policy ties cyber defenses with more mainstream efforts through a new and permanent Defence Policy and Planning Committee in Reinforced format or DPPC(R) to manage the overall NATO planning process, including cyber capabilities. The "Reinforced" in the name means it is chaired by the Deputy Secretary General (rather than an Assistant Secretary General) and the regular membership is augmented, as needed, by others organizations, such as the Budget or Intelligence Committees or the board of the NATO Consultation, Command and Control Agency. The DPPC(R) oversees the work of the CDMB to better ensure the policy and action plan are receiving proper attention and funding from NATO and national members. (See Box 4.)

Perhaps most importantly of all, the new cyber policy has given clarity to the process the Alliance will use to invoke collective defense while maintaining ambiguity about specific thresholds. This process for escalation begins at the technical level. If an incident has political implications, these get escalated from the NCIRC to the CDMB and DPPC(R) through to the North Atlantic Council, the most senior political body, under the guidance of their national leaders.

Box 4: Select NATO Cyber Organizations

HQ NATO Emerging Security Challenges Division
"Deals with the growing range of non-traditional risks and security challenges such as terrorism, the proliferation of WMD, nuclear policy, cyber defense and energy security"

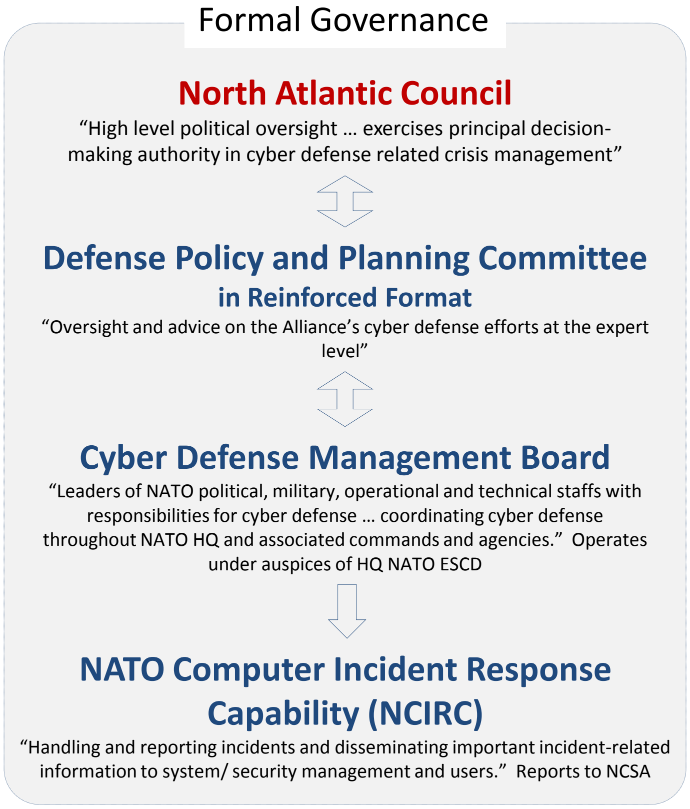
NATO Communication and Information Systems Services Agency (NCSA)
"Responsible for provision of technical and operational cyber security services throughout NATO" and oversees NCIRC

NATO C3 Board
"Governing body for the NC3A"

NATO C3 Agency (NC3A)
"Responsibilities for identifying … operational requirements and acquisition and implementation of NATO's cyber defense capabilities." "The NATO agency responsible for building the new cyber defenses"

Allied Command Transformation
"Takes new operational concept …, assess their viability and value, and brings them to maturity through doctrine development, scientific research, experimentation and technological development." Oversees CCDCOE

Cooperative Cyber Defense Center of Excellence
"Enhance the capability, cooperation and information sharing … in cyber defense through education, research and development, lessons learned and consultation"



Formal Governance

North Atlantic Council
"High level political oversight … exercises principal decision-making authority in cyber defense related crisis management"

Defense Policy and Planning Committee in Reinforced Format
"Oversight and advice on the Alliance's cyber defense efforts at the expert level"

Cyber Defense Management Board
"Leaders of NATO political, military, operational and technical staffs with responsibilities for cyber defense … coordinating cyber defense throughout NATO HQ and associated commands and agencies." Operates under auspices of HQ NATO ESCD

NATO Computer Incident Response Capability (NCIRC)
"Handling and reporting incidents and disseminating important incident-related information to system/ security management and users." Reports to NCSA

Sources: Various official NATO and NATO PA websites

The new NATO policy does not get into further detail on what happens next but the process would likely be similar to response for any other kind of event. Any nation in the Alliance can also call a formal consultation with the other Allies, under Article 4 of the Washington Treaty, if they feel their security is threatened, including by a cyber incident. While this may seem obvious to people that understand NATO decision making, it is often misunderstood who see cyber conflict as a mainly technical issue.

If the incident were especially devastating, the North Atlantic Council could also choose to invoke collective defense through Article 5, a process which could happen quickly. Within twenty-four hours, the North Atlantic Council determined that the 9/11 terrorist strike against the United States was an armed attack and externally directed (not domestic) and decided that aircraft could be used as weapons. Accordingly, NATO rapidly invoked Article 5 for the very first time.

Though the defense ministers confirmed that NATO would "maintain ambiguity" about responding to cyber attacks, it is very unlikely the North Atlantic Council would invoke collective defense unless there were significant damage and deaths, equivalent to kinetic military force. This is a similar process that worked for responding to 9/11, which was considered successful and timely. If a cyber attack is part of a larger crisis however, such as part of a traditional military conflict, NATO will rely on its existing crisis management procedures. (See Box 6 for more on the criteria of what cyber incidents might trigger Article 5.)

The Alliance is also expanding its defenses in 2012, spending 28 million euros to improve its ability to detect attacks, react to them, and provide reaction teams improved equipment. NATO continues conducts frequent cyber exercises. According to the Secretary General, "The most recent Cyber Coalition 2011 exercise included six partners: Finland and Sweden were players, and Australia, Austria, Ireland and New Zealand sent observers, as did the European Union."

Box 5: NATO's Cyber Future: The Alliance's Cyber Deterrence

Though cyber deterrence is a much discussed topic, the most important point is straightforward: NATO should follow the US Department of Defense lead and focus on deterrence by denial. Defenses before an attack, and responses after, should be effective enough so that potential adversaries know they may not be able to achieve their intended effects. The strong defensive and response measures in the current NATO Cyber Defence Policy can, if implemented, be a strong deterrent, denying benefits to potential adversaries so they are dissuaded from attacking in the first place.

The Alliance may also achieve deterrence by punishment in several ways.

1. Any nation choosing another major attack even on a small Ally, such as Estonia, now knows there is a very well-understood path for NATO's political leadership to escalate the situation to an Article 4 consultation or Article 5 invocation of collective defense.

2. Both the White House and Pentagon have been extremely clear that Alliance commitments extend to major cyber attacks.

3. Though NATO does not have an offensive cyber capability, several member nations do have those capabilities which could be used in response.

Neither this deterrence by denial nor punishment provide certainty against future attacks. However, any national leadership will now face a very different calculus than when Estonia was attacked in 2007.

NATO's Cyber Future: Key Insights from the Private Sector

While these existing policies advance NATO's strategic cyber capabilities, one of the most important lessons from other organizations is that the Alliance will have to continue to reinvent its capabilities to meet the rapid advancements and innovation of cyber adversaries.

Aim for Security and Resilience Standards: As NATO starts to address a wider range of chaotically interrelated problems (including governance, policy, incident response, security and resilience) it can fortunately adopt or adapt one of several existing approaches to simplify the process and reduce costs. These will set common baselines for all NATO member militaries, making it clear the expectations for each. Though the most obvious approach is the widely accepted international standards, more recent work on resilience also has advantages.

ISO/IEC 27001 and 27002 are the main international standards for information security to assist organizations to assess risks and design management and technical systems to deal with those risks. With best practice recommendations across twelve areas (including risk assessment, security policy, asset management, human resources, physical security, access control, incident management, and business continuity), these standards would be a significant step forward for NATO. Moreover, they are widely understood, recognized worldwide, and have a directly equivalent national standard in many NATO countries, which could speed acceptance and implementation.

The Resilience Management Model from the Computer Emergency Response Team at Carnegie Mellon University (a pioneer in the field of computer security) is much newer and accordingly not as understood or accepted. However RMM brings other advantages, as it focuses not just on the security but also the resilience of systems, especially during crises. The appraisal process "determines not only whether the organization is doing the *right things right now*, but whether it is capable of sustaining an acceptable level of performance during times of stress and over the long run." A focus on performance during crisis events seems to be an extremely useful approach for an organization preparing for potential combat when opponents will probe to find the least secure and resilient systems.

Moreover, RMM helps define the maturity level of the organization and help it move from ad hoc muddling through to "performing with an emphasis on predictable, repeatable, and consistent results."

Whether NATO chooses to pursue the ISO/IEC standards or RMM, either one can mature NATO cyber capabilities

Box 6: NATO's Cyber Future: Article 5 and Cyber Incidents

The exact criteria of which cyber incidents may trigger an Article 5 invocation of collective defense have not been determined. However, the North Atlantic Council is very likely to consider these elements in its deliberations:

Scope: Is the incident widespread across a wide geographic area or industrial sectors? The wider the attack is, the more likely NATO action will be.

Duration: Is the incident a single event or does it last over time, such as part of a longer campaign? NATO is more likely to act for extended incidents.

Intensity: Has the incident caused death or substantial property destruction? If not, NATO is unlikely to declare collective defense.

External Actor: Is the incident directed from a foreign or domestic adversary? NATO is unlikely to act against a purely domestic foe.

The first three elements are from Thomas Wingfield, an international lawyer, and have become the basic test to determine if a cyber attack rises to the level of an "armed attack" under the UN Charter. The last is particular to NATO, based on response to previous events like the 9/11 attacks on the United States.

and help harmonize national militaries. According to Chris Fogle, a former US Air Force officer who has worked with NATO and has experience with both ISO and RMM, either would be useful: "ISO is a set of standards, built on experience and reflecting expert opinion. RMM is derived from multiple standards, with best practices and typical work products to implement them. In a way, RMM incorporates ISO but would likely be harder to deploy, especially in a large multinational organization like NATO."

Sticking to the Basics: The most noteworthy strength of NATO's new cyber strategy is its focus on defense, rooted in the necessary missions of coordination, training, and defense. Moreover, it recognizes that many of the most significant cyber problems can be solved with smart policies, governance and processes rather than an over-reliance on technology. This very reasonable start must be followed up by execution of the plan itself, for which an action plan is now being drawn up in NATO headquarters. One of the most important actions will be continue to strengthen incident response, particularly via the NCIRC.

NCIRC, the incident response center at the core of NATO's cyber defense, has not yet achieved its full operational capability. It only extends its umbrella of protection to NATO's military wing, so that civilian agencies (like the NATO Defense College or the Disaster Relief Coordination Center) cannot rely on NCIRC to help monitor their systems or respond to incidents. Additionally, NCIRC is seemingly not staffed to handle some of the most important aspects of response, such as coordination with law enforcement, which has been handled by the policy-focused cyber office of the Emerging Security Challenges Division. This is out of line with the standard practice (much less *best* practice) of having law enforcement liaison officers integrated with incident response. As US Department of Defense recognized and largely solved this issue back in 1998, creating a law enforcement and counterintelligence cell in the newly formed Joint Task Force for Computer Network Defense, there is no reason for NATO to relearn old lessons.

As both the ISO/IEC standards or the Resilience Maturity Model, discussed above, highlight both standard and best defensive practices, either will help NATO further stick to the basics of defense.

Should NATO Have an Offensive Capability? Since NATO is a military organization, it seems natural to consider if it should have offensive capabilities in addition to these defensive ones. Indeed, an offensive cyber operation in support of NATO appears to already have been considered. According to the New York Times, in early 2011 the Obama administration and military commanders considered "a cyberoffensive to disrupt and even disable the Qaddafi government's air-defense system." The response to this story seemed to be misplaced surprise that cyber capabilities were at all considered even though military leadership would be negligent if they did not ask about cyber options:

Cyber capabilities may be able to provide military commanders the capability not only to limit the risk to their own forces but also to limit civilian casualties and damage to critical infrastructure. If cyber capabilities could disable Libyan air defenses from afar (as we are told the Israelis may have done to the Syrians in 2007), then a military commander would be reckless to rule out cyber capabilities without even considering them. Cyber capabilities are not nuclear weapons, usable only as a last resort. Most – especially those targeted at battlefield systems not connected to the Internet – are far more precise.

The cyber capabilities discussed in the New York Times story are not organic NATO assets. If they would have been used, it likely would have been conducted as a separate operation to support NATO but outside of its formal chain of command. NATO would officially know there would be an effect, along with a location and time, but probably not any of the operational details. In this sense a "NATO offensive capability" already exists, but it lies within the national militaries, not in any collective NATO agency or unit.

Recommendations

To develop cyber capabilities, NATO should focus its efforts on the following areas. These first seven recommendations are general and could apply to any military organization facing challenges in cyberspace.

1. **Pursue a relevant standard**, such as the widely understood ISO/IEC 27001 and 27002 or the newer RMM, which has more focus on performance during crises.

2. **Invest resources in the basics**. Incident response, information sharing, resilience, properly maintaining computers to "patch" them from being vulnerable, and generally executing the new strategy.

3. **Emphasize agility**. It was only fifteen years from the first flight of an airplane to the battle of Saint-Mihiel, the first coordinated air operation, under a single commander and in support of a ground attack. Though we have over twice that many years experience in cyberspace, we do not yet have a similar understanding of what cyber conflict will eventually look like or how national militaries – much less NATO – should organize for it. This means militaries will need to remain agile. Options might include a heavier than normal reliance on capabilities from national members; learning to quickly procure and secure commercial IT systems; pooling and sharing; and collaboration with the private sector (see below).

4. **Learn to fight through intrusions**. Neither NATO, nor the militaries of its member nations, will be able to keep adversaries from intruding during a cyber conflict. As stated in the new US Department of Defense cyber strategy: "Operating with a presumption of breach will require DoD to be agile and resilient, focusing its efforts on mission assurance and the preservation of critical operating capability." In line with the 2009 Strasbourg Summit Declaration, NATO exercises must fully integrate cyber into all its exercises and train to work through disruptions. Just as air forces must fly and fight through hostile jamming, so must militaries also be able to operate when adversaries are inside their perimeter in cyberspace.

5. **Develop and research advanced capability** to stay ahead of the evolving threats. Investment into research and the next generation of security intelligence capability is needed but advanced security analytics – coupled with automation – will be required including through the existing Science for Peace and Security Program.

6. **Develop an agenda for private sector collaboration**, not just for information sharing, but in more substantive ways as well. Many non-governmental organizations have significant capabilities to fight cyber crime, respond to incidents, and foster cooperation with other nations, making it productive and cost effective for NATO to collaborate. While the current policy says that NATO "will work with partners, international organizations, academia, and the private sector in a way that promotes complementarity and avoids duplication," this actually requires agility, fresh thinking and, above all, a plan to tie together efforts like the existing Framework for Collaborative Interaction, established by NATO's Allied Command Transformation.

7. **Treat cyber conflict as a national security problem** for policymakers, not just a technical issue for computer

security professionals. Policy makers must demand options that do not rely on exact attribution, such as ratcheting pressure against national leaders that encourage attacks, whether or not those attacks can be traced to that nation's infrastructure. In addition, at the Chicago Summit of 2012, NATO should support important cyber norms, such as that any alliance cyber operations will conform to the Laws of Armed Conflict and that NATO will not use or encourage third-party, non-state proxies to conduct cyber attacks on its behalf.

The following ideas are specific to NATO:

8. **Explore how a "phased adaptive" approach might apply to cyber defense**. Though the parallels to missile defense are imperfect, NATO should consider structuring their future cyber defense plans into multiple phases depending on future threats and technologies. Phase 1 might improve NATO's own defenses, while Phase 2 extends these to national militaries. Later phases could include sharing information with the EU, infrastructure providers, or erecting a cyber umbrella of warning and defenses.

9. **Push multinational sharing of baseline capabilities**. NATO may not need a separate IT schoolhouse for each nation's military or service or separate national IT procurement programs, as Allies use the same Internet for similar purposes and purchase generally identical computers and switches. If nations can share aircraft carriers then there are likely obvious options to share and pool cyber capabilities.

10. **Rely on the European Union**, especially for issues such as the resilience of national infrastructure, on which NATO militaries rely. Likewise, the EU might rely on NATO to harmonize national military efforts and engage the capabilities (and better instincts) of the United States.

11. **Tie in to civilian ministries**. In many NATO nations, civilian organizations (such as the crime fighters in Interior ministries) have the most cyber resources and are have the national role to coordinate cyber defenses. Whether through the EU, or through the new or existing military links, NATO must develop a mechanism in the medium term to connect military and civilian ministries.

12. **Consider offensive coordination, not capability**. When the US military started exploring offensive cyber capabilities, it began with small, embedded units who knew both traditional and cyber military operations – and had the proper clearances. During future crises NATO might consider creating an ad hoc coordination cell. These officers should apply, but not necessarily share, their knowledge of sensitive capabilities to help communicate the objectives of the Alliance's operational commanders to their relevant national cyber units. This coordination group might be similar to the US Air Forces Cyber Operations Liaison Element. In addition, as suggested by the Atlantic Council's Franklin Miller, NATO should consider creating a group, modeled on NATO's existing Nuclear Planning Group, to consider offensive cyber policy.

Conclusion

The challenges NATO faces will not slacken and budgets will continue to shrink. The recommendations in this Issue Brief will help ensure that NATO is as successful in cyberspace as it is in the domains of air, land, maritime, and space. None of these recommendations embody new capabilities, but reflect the realities of modern military missions combined with smart defense for a smarter Alliance.

FEBRUARY 2012

The Atlantic Council's Board of Directors

CHAIRMAN

*Chuck Hagel

CHAIRMAN, INTERNATIONAL ADVISORY BOARD

Brent Scowcroft

PRESIDENT AND CEO

*Frederick Kempe

VICE CHAIRS

*Richard Edelman
*Brian C. McK. Henderson
*Richard L. Lawson
*Virginia A. Mulberger
*W. DeVier Pierson

TREASURERS

*Ronald M. Freeman
*John D. Macomber

SECRETARY

*Walter B. Slocombe

DIRECTORS

*Robert J. Abernethy
Odeh Aburdene
Timothy D. Adams
Carol C. Adelman
Herbert M. Allison, Jr.
Michael A. Almond
*Michael Ansari
Richard L. Armitage
Adrienne Arsht
*David D. Aufhauser
Ziad Baba
Ralph Bahna
Lisa B. Barry
*Thomas L. Blair
Julia Chang Bloch
Dan W. Burns
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Daniel W. Christman
Wesley K. Clark
John Craddock
Tom Craren
*Ralph D. Crosby, Jr.
Thomas M. Culligan
Gregory R. Dahlberg
Brian D. Dailey
*Paula Dobriansky
Markus Dohle
Lacey Neuhaus Dorn
Conrado Dornier
Patrick J. Durkin
Eric S. Edelman
Thomas J. Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Dan-Åke Enstedt
Julie Finley
Lawrence P. Fisher, II
Barbara Hackman Franklin
*Chas W. Freeman
Jacques S. Gansler
*Robert Gelbard
Richard L. Gelfond
*Edmund P. Giambastiani, Jr.
*Sherri W. Goodman
John A. Gordon
*C. Boyden Gray
*Stephen J. Hadley
Mikael Hagström
Ian Hague
Rita E. Hauser
Annette Heuser
Marten H.A. van Heuven
*Mary L. Howell
Benjamin Huberman
Linda Hudson
*Robert E. Hunter
Robert L. Hutchings
Wolfgang Ischinger
Robert Jeffrey
*James L. Jones, Jr.
George A. Joulwan
Stephen R. Kappes
Francis J. Kelly
L. Kevin Kelly
Zalmay Khalilzad
Robert M. Kimmitt
*Roger Kirk
Henry A. Kissinger
Franklin D. Kramer
Philip Lader
David Levy
Henrik Liljegren
*Jan M. Lodal
George Lund
Izzat Majeed
Wendy W. Makins
William E. Mayer
Barry R. McCaffrey
Eric D.K. Melby
Rich Merski
Franklin C. Miller
*Judith A. Miller
Alexander V. Mirtchev
Obie Moore
*George E. Moose
Georgette Mosbacher
Bruce Mosler
Sean O'Keefe
Hilda Ochoa-Brillembourg
Philip A. Odeen
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 Roth
Michael L. Ryan
Harry Sachinis
Marjorie M. Scardino
William O. Schmieder
John P. Schmitz
Jill A. Schuker
Kiron K. Skinner
Anne-Marie Slaughter
Alan Spence
John M. Spratt, Jr.
Richard J.A. Steele
Jim Steinberg
Philip Stephenson
*Paula Stern
John Studzinski
William H. Taft, IV
John S. Tanner
Peter J. Tanous
Paul Twomey
Henry G. Ulrich, III
Enzo Viscusi
Charles F. Wald
Jay Walker
Michael Walsh
Mark R. Warner
J. Robinson West
John C. Whitehead
David A. Wilson
Maciej Witucki
R. James Woolsey
Dov S. Zakheim
Anthony C. Zinni

HONORARY DIRECTORS

David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
James R. Schlesinger
George P. Shultz
John Warner
William H. Webster

LIFETIME DIRECTORS

Lucy Wilson Benson
Daniel J. Callahan, III
Kenneth W. Dam
Stanley Ebner
Carlton W. Fulford, Jr.
Geraldine S. Kunstadter
James P. McCarthy
Jack N. Merritt
Steven Muller
Stanley R. Resor
William Y. Smith
Helmut Sonnenfeldt
Ronald P. Verdicchio
Carl E. Vuono
Togo D. West, Jr.

* Members of the Executive Committee
List as of February 21, 2012

The Atlantic Council is a non-partisan 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