Atlantic Council
BRENT SCOWCROFT CENTER
ON INTERNATIONAL SECURITY

ISSUEBRIEF

BY JASON HEALEY AND KLARA TOTHOVA JORDAN

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

SEPTEMBER 2014

NATO's central missions of collective defense and cooperative security must be as effective in cyberspace as in the other domains of air, land, sea, and space.

The Alliance formulated its mission in cyberspace—to protect its own networks, enhance the capabilities of the member states, and to cooperate with partner nations, the European Union (EU), and industry—after suffering its first major cyberattacks in 1999, during Operation Allied Force.

Although the organization matured significantly both in its understanding of the threat and its preparedness to respond to it, NATO is still playing catch up with national cyber defense vulnerabilities. The role of NATO in strengthening the cyber defenses of individual allies has only recently attracted the attention of senior leaders and will be one of the issues debated at the September NATO Summit in Wales, United Kingdom.

The current NATO Policy on Cyber Defense, adopted in 2011, and the Action Plan that followed gave the Alliance a strong boost by prioritizing the defense of NATO's own networks. But the Alliance should now "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 developed in their wake.

The brief then looks at NATO's present, its 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 and provides specific recommendations going forward.

Cyber Statecraft Initiative

The focus of the Cyber Statecraft Initiative is to examine the overlap of national security, international relations, and economic security issues to provide practical and relevant solutions to challenges in cyberspace. The Initiative looks to the past, present, and future of the Internet to convince governments and companies not to become obsessed with short-term gains that put the world's shared digital future at risk.

The Cyber Statecraft Initiative has accordingly made its mission "Saving Cyberspace." The Initiative's many novel ideas and projects help realize this vision in Washington, DC, and other national capitals and technology centers. Cyber statecraft will be a key tool to guide policymakers through the maze of cyberspace.

This issue brief is a significantly updated version of a previous work, coauthored with Leendert van Bochoven, that was conducted as part of the Atlantic Council's Smarter Alliance Initiative in partnership with IBM.

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

Although NATO continued issuing guidance over the years—such as the Prague Capabilities Commitment of

Jason Healey is director and **Klara Tothova Jordan** is assistant director of the Cyber Statecraft Initiative in the Brent Scowcroft Center on International Security.

Box 1. NATO's Cyber Past: Operation Allied Force, 1999

A flurry of cyber incidents against NATO and member governments and militaries occurred during Operation Allied Force in 1999, the goal of which was 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, Serb, and Chinese hackers after the accidental bombing of the Chinese Embassy in Belgrade.

2002 and the Comprehensive Political Guidance of 2005—it was not until the 2007 attacks against Estonia that the Alliance truly realized the technical scale and political implications of potential cyberattacks (see box 2). 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 cyberattack." The NATO Cyber Defense Policy was approved in January 2008 and endorsed at the Bucharest Summit, which helped strengthen NATO's focus on cyber issues.

The Alliance's leadership established two institutions at the Bucharest Summit tasked with implementing and supporting the objectives laid out in the Cyber Defense Policy: 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 (CDMB)—became fully operational in April 2008 with the mission to initiate and coordinate cyber defenses, review capabilities, and conduct appropriate security risk management. The CDMA also helps member states improve their own national cyber defense capabilities. The CDMA has been replaced by the CDMB with responsibility coordinating cyber defense throughout NATO's civilian and military bodies.

The CCDCOE based in Tallinn, Estonia, does not have an operational cyber mission. Its main role is to support the Alliance and member nations through the improvement of interoperability and capabilities, doctrine development, education, and training. The Tallinn center has been particularly influential in legal issues by convening together practicing lawyers and academics from around the Alliance.

In response to demands for a capability to assist allies seeking NATO's support in protection or response, NATO stood up two Rapid Reaction Teams (RRTs) that can help protect and troubleshoot NATO and national networks in the event of an attack. While the RRTs provide only limited technical assistance (helping to protect and restore systems or coordinating the response), their main value is political, displaying the Alliance's commitment to support its own systems and the attacked ally, both within the Alliance and to the leadership of nations sponsoring or conducting the attacks.

NATO's Strategic Concept and the 2010 Lisbon Summit Declaration continued the 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 cyberattack. To this end, the Lisbon Capabilities Package addressed the most pressing gaps, including improvements to the NCIRC.

On the political level, the Lisbon Summit mandated the integration of cyber defense into NATO's Defense Planning Process (NDPP), and the heads of state committed to a revised NATO cyber defense policy. With these steps, NATO aimed to pave the way for capabilities that would allow the Alliance to fully integrate cyber into its collective defense, crisis management, and cooperative security mission.

NATO's Cyber Present

The Cyber Defense Policy and the Action Plan of June 2011 are by far the most important actions the Alliance has taken so far to mature its cyber capabilities and governance structures. Approved while NATO was conducting air operations over Libya (see box 3), both

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 flooding networks or websites with attack traffic, rendering them inaccessible.

The attacks—many of which came from Russia, written in Russian, or coordinated from 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 the Kremlin.

Box 3. NATO'S Cyber Past: Operation Unified Protector, 2011 and the Rise in Cyber Threats

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

- The group Anonymous publicly warning NATO not to challenge it after a report on hacktivism specifically mentioned the group; Anonymous then claimed to have intruded into a NATO server and extracted a large amount of data.
- 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 twelve thousand registered users.
- The Norwegian military reported suffering a malicious software attack one day after the beginning of NATO bombing operations in Libya.

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

documents aimed to enhance the political and operational mechanism of NATO's response capability, and expand training and assistance to improve Alliance defenses and national capabilities. The main elements of the approach include:

- realization that cyber defense is required to perform NATO's core tasks of collective defense and crisis management;
- prevention, resilience, and defense of cyber assets critical to NATO and its constituent allies;
- implementation of robust cyber defense capabilities and centralized protection of NATO's own networks;
- definition of minimum requirements for cyber defense of national networks critical to NATO's core tasks;
- assistance to the allies to achieve a minimum level of cyber defense to reduce vulnerabilities of national critical infrastructure; and
- engagement with partners, other international organizations, the private sector, and academia.

To implement these new policies and capabilities, NATO's main governance body for cyber defense, the Cyber Defense Management Board (CDMB), has been signing Memoranda of Understanding with the appropriate authority in each member nation. As of August 2014, twenty-seven such agreements have been signed. Progress will be reported "regularly" to the Alliance's highest political body, the North Atlantic Council (NAC).

In addition, the policy ties cyber defense with more mainstream efforts through a new and permanent Cyber Defense Committee (CDC) to manage political governance and cyber defense policy in general, including cyber capabilities. The committee provides oversight and advice to allied nations on NATO's cyber defense efforts at the expert level (see box 4).

Perhaps most importantly, the cyber policy has given clarity to the process the Alliance will use to fulfill its collective defense mission while maintaining ambiguity about specific thresholds.

This process for engagement begins at the technical level. If an incident has political implications, NATO's cyber defense efforts get elevated from the NCIRC to the CDMB and CDC through to the NAC.

The NATO policy does not go into further detail about what happens next but the process would likely be similar to the response to 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 it feels its territorial integrity, political independence, or security is threatened, including by a cyber incident. While this may seem obvious to people who understand NATO decision-making, it is often misunderstood by those who see cyber conflict as a mainly technical issue.

If the incident was especially devastating, the NAC could also choose to invoke collective defense through Article 5, a process which happened quickly after the terrorist attacks on 9/11. The 2010 Strategic Concept revealed the political backing to the applicability of the concept of collective defense to the cyber domain. The Strategic Concept stated, in essence, that a cyberattack against member states could justify them turning to NATO for assistance or invoking Article 5 of the Washington Treaty. In the case of 9/11 attacks, the NAC determined that the 9/11 terrorist strike against the United States was an externally directed (not domestic) armed attack and decided that the use of aircraft could be considered similar to the use of a weapon. Accordingly, NATO invoked Article 5 within twenty-four hours for the first time in its history.

Box 4. NATO Cyber Defense Stakeholders

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

NATO Communication and Information Agency (NCIA)
Through NCIRC Technical Center, it assumes the Alliance's cyber defense and provides analysis and concept development through experimentation and capability development in cyber defense. NC3A was merged into NCIA in July 2012.

NATO C3 Board
Multinational policy body in the consultation, command, and control area.

Allied Command Transformation
Responsible for doctrine development, scientific research, experimentation, and technological development. Assesses the viability and value of new operational concepts. NATO coordinates the work of CCD COE via ACT.

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

Formal Governance

North Atlantic Council
Principal political decision-making authority for policy and operational questions requiring collective decisions in the cyber defense area.

↕

Cyber Defense Committee
The lead committee for political governance and cyber defence policy in general, providing oversight and advice to allied nations on NATO's cyber defense efforts at the expert level.

↕

Cyber Defense Management Board
Assembles leaders of NATO political, military, operational, and technical staffs with responsibilities for cyber defense. The board coordinates cyber defense throughout NATO civilian and military bodies. Operates under auspices of HQ NATO ESCD.

↕

NATO Computer Incident Response Capability (NCIRC)
Provides centralized protection and round the clock cyber defence support to NATO static and deployed HQs, agencies, and national networks.

Source: Various official NATO and NATO PA websites.

Though the defense ministers confirmed that NATO would "maintain ambiguity" about responding to cyberattacks, it is very unlikely the NAC would invoke collective defense unless there were significant kinetic effects such as damage and deaths. This is a similar approach to the one applied in response to the 9/11 attacks, which was considered successful and timely. However, if a cyberattack is part of a larger crisis, such as part of a traditional military conflict, NATO will most likely rely on its existing crisis management procedures (see box 7 for more information on criteria of cyber incidents that might trigger Article 5).

The Alliance also invested in expanding its defenses in 2012, committing to spend 58 million euros to improve its ability to detect cyberattacks and react to them by upgrading the Computer Incident Response Capability (NCIRC). The capability provides a centralized protection through state-of-the-art sensors and scanners of fifty-one sites, covering NATO's static and operational headquarters and agencies.

In 2012, NATO also created a cyber threat assessment cell with the mission to analyze the most significant cyber threats.

NATO continues to conduct frequent cyber exercises. The latest two—Cyber Coalition, conducted in 2013, and Locked Shields in 2014—exhibit growing scale and sophistication, both in terms of evolving scenarios and number of participants. Exercises are the backbone of NATO's strategy to test concepts and strategies and support building interoperability among the allies. In the cyber arena, they allow, in particular, testing incident response and crisis management procedures to cyberattacks.

In 2013, NATO took an additional set of political and operational steps to enhance the Alliance's capabilities to defeat cyberattacks and raised the issue to the top of its security agenda.

At the political level, at the first NATO Defense Ministerials solely dedicated to cyber defense, the ministers agreed to strengthen the organization's cyber defenses by extending protection to all the networks owned and operated by the Alliance and including cyber defense in NATO's defense planning process.

At the operational level, the Smart Defense portfolio was broadened by three projects. The Multinational Cyber Defense Capability Development project aims to improve the means for sharing technical information and promotes awareness of threats and attacks. The Malware Information Sharing Platform (MISP) aims to develop a NATO capability, available to all NATO nations,

through which nations commit to sharing information of the technical characteristics of malware without the necessity to share details of the attack. The third project, focusing on training and education, streamlines education in the area of technical, operational, strategy, and policy elements of cyber defense throughout a network of educational institutions such as NATO Scholl Oberammergau, NATO Communications and Information Systems School (NCISS) in Latina, Italy (planned to relocate to Portugal), and NATO CCD COE.

In recent years, the cyber threat to NATO has been growing, both in scale and sophistication. In 2013 NATO defenses dealt with over 2,500 significant cases of cyberattacks. During the peak of the tensions over Crimea in March 2014, several public NATO websites were brought down by distributed denial-of-service (DDoS) attacks. Although the incidents were described as "significant" by the organization, they were mild disturbances without the capacity to disrupt military command and control.

Despite the challenges NATO faces, not least controversy over burden sharing and inequalities in member states' capabilities, it is taking the next step toward cyber maturity.

Endorsed in June 2014 by NATO defense ministers, the new Enhanced NATO Policy on Cyber Defense and its implementation plan will be announced at the NATO Summit in September. The progress of the organization in the cyber defense arena is demonstrated by the fact that unlike with past policy developments, no one significant cyber crisis prompted the organization to revisit its cyber defense posture.

The new policy is expected to advance the governance of cyber defense in the organization, introduce a new approach to collaboration with industry via NATO Industry Cyber Partnership (NICP), reinforce the framework for capability development of individual allies, and place reinforced emphasis on training and education. NATO is maturing to understand that it is very hard to keep a dedicated attacker out of the system and, therefore, resilience of its own and of national systems and defenses is the way to secure its strategic objectives.

Another significant point in the new policy is the clear statement that cyber defense is linked to collective defense and that international law applies in cyberspace. Despite the fact that both of these positions have already been voiced, this is the first time NATO as an organization included them in a policy document in the cyber defense arena. The clear pronouncement on applicability of collective defense to the cyber domain is an important reassurance and deterrent measure, one that is long overdue given that every conflict now has a cyber element.

Box 5. NATO's Cyber Present: Recent Confrontations, 2014

Although thousands of relatively minor attacks against NATO are carried out each month at a growing rate, the number of large-scale attacks directed against the Alliance or its affiliated partners have been relatively low with a few exceptions:

In March of 2014, pro-Russian hacktivists brought down several NATO websites in an attack that was linked to the escalating crisis in Crimea. NATO's public websites, as well as NATO unclassified email network and the CCDCOE, were targeted. No critical or classified systems were reportedly affected. Nevertheless, the attack was one of the most significant cyber strikes against the Alliance in years.

Physical conflict begets cyber conflict, and while these attacks were not detrimental to any crucial systems or infrastructure, they are indicative of real opposition to NATO and its partner entities. NATO, however, has publicly regarded these attacks more as technical setbacks than as notable aggressions.

Over the course of the past decade, NATO has created capabilities that have secured the organization's own networks relatively well and set up a framework to support the capability and capacity building of the allies. However, the organization is still catching up on an ever-growing threat given the organization's size, importance, and mission. There are several areas where the organization could level the playing field with malicious actors.

Recommendations for NATO's Cyber Future

In order to develop cyber capabilities, NATO should focus its efforts on the following areas. The first five recommendations are generic and could apply to any military organization facing challenges in cyberspace.

- **Stick 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 with execution of the strategy itself, for which an action plan is now being drawn up at NATO headquarters. One of the most important actions

Box 6. 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 goals. The strong defensive and response measures in the current NATO Cyber Defense 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.

- 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.
- Both the White House and Pentagon have been extremely clear that Alliance commitments extend to major cyberattacks.
- Though NATO does not have an offensive cyber capability, several member nations do have those capabilities that could be used in response.

will be continuing to strengthen incident response, particularly via the NCIRC, and supporting the development of member states' capabilities.

- **Pursue a relevant standard** such as the widely understood ISO/IEC 27001 and 27002 or the newer Resilience Management Model (RMM), which has more focus on resilience and performance during crises.
- **Fight through cyberattacks**: Perhaps the best outcome of the Wales Summit would be an equivalent cyber strategy that commits not only to keeping attackers out, but to carry on through intrusions and other attacks, and not let them rise to become NAC issues. Just as air forces must fly and fight through hostile jamming without first seeking NAC approval, so should militaries also be able to react and operate when adversaries are inside their perimeter in cyberspace, during a so-called "presumption of breach." This could be achieved through resiliency plans and exercises, specialized incident response teams, and redundant basting for government and critical infrastructure sites.
- **Develop an agenda for private sector collaboration:** Collaboration with the private sector should not just focus on information sharing, but on other, more substantive issues as well. Many nongovernmental 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 new policy states that NATO will reinforce its relationships with industry and facilitate voluntary engagement between NATO and industry, 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.
- **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. A great example of this kind of cooperation is the Estonian cyber rang where NATO and its nations have been provided access to.
- **Reinforce coordination with the European Union**: This would be especially valuable for issues such as the resilience of national infrastructure, on which NATO militaries rely through closer relationship with ENISA. The EU should be part of NATO's exercises involving critical infrastructure operators. Likewise, the EU might rely on NATO to harmonize national military efforts and engage the capabilities of the United States.
- **Consider offensive coordination, not capability**: When the US military started exploring offensive cyber capabilities, it began with small, embedded units that were knowledgeable about both traditional and cyber military operations—and had the proper clearances. During future crises, NATO might consider creating an ad hoc coordination cell, where officers would 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

Atlantic Council Board Director Franklin Miller, NATO should consider creating a group, with voluntary opt-in for states, modeled after NATO's existing Nuclear Planning Group, to discuss and map out an offensive cyber policy.

- **Focus on Articles 4 and 5**: Despite the mystique build around it, cyber conflict need not be particularly technical or mysterious. One finding of the first-ever military history of cyber space, *A Fierce Domain: Cyber Conflict, 1986 to 2012*, is that the more strategically significant the cyber conflict, the more similar it is to conflict in other domains.[1] Any likely Article 4 and 5 response from a cyberattack is therefore extremely likely to take place during an existing geopolitical crisis with a known national rival. A very modest effort could examine the information, decisions, and actions needed to be ready when these situations arise, and reinforcing this with supporting exercises.

- **Be prepared for attribution**: Despite the frustration of not knowing who is behind cyber crimes, the nation responsible for national security cyberattacks is usually quite obvious. NATO leaders could be reasonably certain that in Crimea the "little green men" with advanced weapons were there because the Russian leadership sent them. Cyberattacks during a geopolitical crisis are simply an online version of these "little green men." The larger problem is the same in both situations: what to do without ignoring aggression or escalating recklessly.

- **Support beyond RRTs**: In addition to the Alliance's existing Rapid Reaction Teams, there is a very wide range of actions the organization could take to help a member nation under sustained assault (of below Article 5 nature)—for example, organizing a coordination cell for cyber crises leveraging the Alliance's full response capabilities. These could be as simple as providing satellite phones or prioritizing bandwidth to ease coordination issues, improved intelligence sharing, or better cooperation between civilian telecommunications providers. During a cyber crisis, there is a shortage of adept project managers, and those roles could be filled by military officers and noncommissioned officers (NCOs) from across the Alliance. It is easy to imagine other actions that could be in the Alliance's playbook. Nearly every cyber conflict in history has been decisively resolved not by governments but by the private sector. Most of the largest IT companies in the world are headquartered in NATO countries, all of which could have a role to play supporting an Alliance member under attack if asked (or funded) by the larger members. Of course, all of this should be supplementary to the more technical incident response specialists and true cyber defenders who could be part of the RRT.

- **IT pooling and sharing**: As an extension of Smart Defense, NATO could decide at the next summit to improve defenses and cut costs by combining members' national military IT structures. If Belgium and the Netherlands can permanently pool fleets and support naval structures, then why couldn't nations do the same with IT procurement contracts, use of cloud computing and storage, and common IT schoolhouses? The basics of cyberspace (networking standards, networking gear, routers and switches, desktop computers, and office software) are the same around the entire Alliance. As part of a truly Smart Defense, nations should find a way to organize, train, equip, and operate these technologies together.

Box 7. NATO's Cyber Future: Article 5 and Cyber Attacks

The exact criteria by 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 geographic area or industrial sectors? The wider the attack, the more likely NATO action will be.

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

Intensity/Scale: 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.

Conclusion

The challenges NATO faces will not decrease while budgets continue to shrink. The recommendations presented in this issue brief should 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 require new capabilities, but reflect the realities of modern military missions combined with Smart Defense for a smarter Alliance.

1 Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986-2012* (Arlington: Cyber Conflict Studies Association, 2013).

Atlantic Council Board of Directors

CHAIRMAN
*Jon M. Huntsman, Jr.

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
*John Studzinski

TREASURER
*Brian C. McK. Henderson

SECRETARY
*Walter B. Slocombe

DIRECTORS
Stephane Abrial
Odeh Aburdene
Peter Ackerman
Timothy D. Adams
John Allen
Michael Ansari
Richard L. Armitage
*Adrienne Arsht
David D. Aufhauser
Elizabeth F. Bagley
Sheila Bair
*Rafic Bizri
*Thomas L. Blair
Francis Bouchard
Myron Brilliant
*R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Ashton B. Carter
James E. Cartwright
Ahmed Charai
Wesley K. Clark
David W. Craig
Tom Craren
*Ralph D. Crosby, Jr.
Nelson Cunningham
Ivo H. Daalder
Gregory R. Dahlberg
*Paula J. Dobriansky
Christopher J. Dodd
Conrado Dornier
Patrick J. Durkin
Thomas J. Edelman
Thomas J. Egan, Jr.
*Stuart E. Eizenstat
Thomas R. Eldridge
Julie Finley
Lawrence P. Fisher, II
Alan H. Fleischmann
Michèle Flournoy
*Ronald M. Freeman
*Robert S. Gelbard
*Sherri W. Goodman
*Stephen J. Hadley
Mikael Hagström
Ian Hague
John D. Harris II
Frank Haun
Michael V. Hayden
Annette Heuser
Marten H.A. van Heuven
Jonas Hjelm
Karl Hopkins
Robert Hormats
*Mary L. Howell
Robert E. Hunter
Wolfgang Ischinger
Reuben Jeffery, III
Robert Jeffrey
*James L. Jones, Jr.
George A. Joulwan
Stephen R. Kappes
Maria Pica Karp
Francis J. Kelly, Jr.
Zalmay M. Khalilzad
Robert M. Kimmitt
Henry A. Kissinger
Peter Kovarcik
Franklin D. Kramer
Philip Lader
*Jan M. Lodal
*George Lund
Jane Holl Lute
*John D. Macomber
Izzat Majeed
Wendy W. Makins
Mian M. Mansha
William E. Mayer
Eric D.K. Melby
Franklin C. Miller
James N. Miller
*Judith A. Miller
*Alexander V. Mirtchev
Obie L. Moore
*George E. Moose
Georgette Mosbacher
Bruce Mosler
Thomas R. Nides
Franco Nuschese
Sean O'Keefe
Hilda Ochoa-Brillembourg
Ahmet Oren
*Ana Palacio
Thomas R. Pickering
*Andrew Prozes
Arnold L. Punaro
*Kirk A. Radke
Teresa M. Ressel
Jeffrey A. Rosen
Charles O. Rossotti
Stanley O. Roth
Robert Rowland
Harry Sachinis
William O. Schmieder
John P. Schmitz
Brent Scowcroft
Anne-Marie Slaughter
Alan J. Spence
John M. Spratt, Jr.
James Stavridis
Richard J.A. Steele
James B. Steinberg
*Paula Stern
Robert J. Stevens
John S. Tanner
Peter J. Tanous
*Ellen O. Tauscher
Karen Tramontano
Clyde C. Tuggle
Paul Twomey
Melanne Verveer
Enzo Viscusi
Charles F. Wald
Jay Walker
Michael F. Walsh
Mark R. Warner
John C. Whitehead
David A. Wilson
Maciej Witucki
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
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
George P. Shultz
John W. Warner
William H. Webster

**Members of the Executive Committee*
^ International Advisory Board Members
List as of May 21, 2014

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.

1030 15th Street, NW, 12th Floor, Washington, DC 20005
(202) 778-4952, AtlanticCouncil.org