GlobalResearch
Center for Research on Globalization

U.S. Cyber Command: Waging War In The World's Fifth Battlespace

By Rick Rozoff

Global Research, May 27, 2010
Stop NATO 26 May 2010

Region: USA
Theme: US NATO War Agenda

On May 21 U.S. Secretary of Defense Robert Gates announced the activation of the Pentagon's first computer command. And the world's first comprehensive, multi-service military cyber operation.

U.S. Cyber Command (CYBERCOM), initially approved on June 23, 2009, attained the status of what the Pentagon calls initial operations capability eleven months afterward. It is to be fully operational later this year.

CYBERCOM is based at Fort Meade, Maryland, which also is home to the National Security Agency (NSA). The head of the NSA and the related Central Security Service is Keith Alexander, U.S. Army lieutenant general on the morning of May 21 but promoted to four-star general before the formal launching of Cyber Command later in the day so as to become its commander.

The U.S. Senate confirmed Alexander for his new position on May 7. In written testimony presented to Congress earlier, he stated that in addition to the defense of computer systems and networks, "the cyber command would be prepared to wage offensive operations as well…" [1] Two days before his confirmation the Associated Press reported that Alexander "said the U.S. is determined to lead the global effort to use computer technology to deter or defeat enemies." [2] The conjunction "and" would serve the purpose better than "or."

The day Alexander assumed his new command Deputy Defense Secretary William Lynn "called the establishment of U.S. Cyber Command at Fort Meade, Md., today a milestone in the United States being able to conduct full-spectrum operations in a new domain," adding that the "cyber domain… is as important as the land, sea, air and space domains to the U.S. military, and protecting military networks is crucial to the Defense Department's success on the battlefield." [3]

The Pentagon's second-in-charge is not the only person to refer to cyber warfare as the world's fifth battleground after those of land, sea, air and space, nor to link the first with the other four.

Indeed, the Defense Department's Quadrennial Defense Review released earlier this year focuses on "a broader range of military responsibilities, including defending space and cyberspace," [4] and the Pentagon's space operations are now grouped with cyber warfare as the new Cyber Command is subsumed under U.S. Strategic Command (USSTRATCOM), which is in charge of the militarization of space as well as the global interceptor missile project, information warfare and related missions.

In its own words, "USSTRATCOM combines the synergy of the U.S. legacy nuclear command and control mission with responsibility for space operations; global strike; Defense Department information operations; global missile defense; and global command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), and combating weapons of mass destruction." [5]

> "U.S. CYBERCOM is a sub-unified command under U.S. Strategic Command, of Offutt Air Force Base in Nebraska. But it will be run out of the super-secretive communications-gathering National Security Agency in Fort Meade, Md." [6]

Three months ago U.S. Air Force Chief of Staff General Norton Schwartz addressed a conference of the Air Force Association, but he "did not mention fighters, special operations or mobility," instead concentrating on space and cyberspace. "We have an enduring need for robust space and cyberspace capabilities," he told the audience.

The Air Force Times provided background information regarding Schwartz's comments and connected the role of space and cyber warfare: "Space and cyberspace missions were brought together last year, when the service moved many of its communications and computer missions into Space Command and created the 24th Air Force to be the service's in-house 'cyber command.'

> "At the same time, Space Command's nuclear missile role was transferred to the new Global Strike Command." [7]

The 24th Air Force will be joined by the Army Forces Cyber Command and the 10th Fleet and Marine Forces Cyber Command (representing the four main branches of the U.S. armed forces) in providing the first 1,000 personnel for the new multi-service Cyber Command.

The day that CYBERCOM was launched, the Pentagon announced that "The U.S. Army will consolidate 21,000 soldiers in its cyber warfare units under a new unified command led by a three-star general." Army Forces Cyber Command, ARFORCYBER, "will be fully operational by October at Fort Belvoir, Va., a sprawling base south of Washington," and will achieve "unprecedented unity of effort and synchronization of Army forces operating within the cyber domain." In the words of the Army's chief cyber commander, Major General Steven Smith, his service is "trying to understand what a cyber warrior should be, and how they should be trained." [8]

A few days before the Air Force revealed that since last November it has transferred at least 30,000 troops from communications and electronics assignments to "the front lines of cyber warfare." [9]

Earlier this month Deputy Under Secretary of Defense for Policy James Miller was cited as maintaining that "The Pentagon would consider a military response in the case of a cyber attack against the United States." He was quoted as proposing a direct military reaction to computer attacks, stating "we need to think about the potential for responses that are not limited to the cyber domain." [10]

Placing computer security, including in the civilian sector, under a military command is yet another step in the direction of militarizing the treatment of what are properly criminal or even merely proprietary and commercial matters. And preparing responses of a decidedly non-virtual nature in return.

The Pentagon and the National Security Agency will not be alone in the endeavor to establish and operate the world's first national cyber warfare command. As usual, Washington is receiving unconditional support from the North Atlantic Treaty Organization, the military bloc it initiated in 1949 and has extended throughout Europe and, operationally, into Asia, Africa and the Middle East over the last eleven years.

NATO not only provides the U.S. with 27 additional voices and votes in the United Nations and as many countries through which to transit and in which to base troops and military equipment, it also – through its Article 5 mutual military assistance provision – allows for American military deployments and creates the pretext for armed confrontation in alleged defense of other member states. Troops from all 28 NATO members and over 20 partner states are embroiled in the nearly nine-year war in Afghanistan because Article 5 was first invoked in September of 2001.

Stating that "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all," Article 5 is in large part the foundation of and the impetus for the Pentagon's Cyber Command.

The clamor for a cyber warfare capacity began among leading American and NATO officials during and immediately after attacks on computer systems in Estonia in late April and early May of 2007. The small country, a neighbor of Russia which had been inducted into NATO three years earlier, accused Russian hackers of the attacks on both government and private networks, and the charge was echoed in the West with the additional insinuation that the government of then Russian President Vladimir Putin was behind the campaign.

Three years later the accusations have not been substantiated, but they have served their purpose nonetheless: NATO dispatched cyber warfare experts to Estonia shortly after the events of 2007 and on May 14, 2008 the military bloc established what it calls the Cooperative Cyber Defence Centre of Excellence (CCD COE) in the nation's capital of Tallinn.

The bloc's Article 5 has been repeatedly – and given its nature ominously – evoked in reference to alleged cyber crimes and attacks, and Estonia has been portrayed as both the model victim of such assaults and the rallying point for a global cyber warfare response to them.

From the genesis of the drive for U.S.-NATO cyber warfare operations Russia has been the clearly implied if not always openly acknowledged target.

In an August 2008 column in the influential Wall Street Journal entitled "Russia's Aggression Is a Challenge to World Order," two leading U.S. senators, Joseph Lieberman and Lindsey Graham, called for "reinvigorating NATO as a military alliance, not just a political one. Contingency planning for the defense of all member states against conventional and unconventional attack, including cyber warfare, needs to be revived. The credibility of Article Five of the NATO Charter – that an attack against one really can and will be treated as an attack against all – needs to be bolstered." [11]

This January U.S.-based Google accused Chinese hackers of "sophisticated cyberattacks" and since then Beijing has joined Moscow as the most frequently cited antagonist in future cyber conflict scenarios, intimately linked to comparable disputes in space over military and civilian satellites.

The British House of Lords issued a report in mid-March of this year that explicitly asserted "Britain needs to work more closely with Nato to fend off 'cyber warfare' on critical national infrastructure from former cold war enemies such as Russia and China," and which "highlight[ed] the dangers of attacks on the internet, banking and mobile phone networks by the Russians in Estonia three years ago." [12]

A few days before NATO Secretary General Anders Fogh Rasmussen, while promoting the military bloc's new Strategic Concept in nominally non-aligned Finland, reiterated that although Article 5 military defense of the Alliance's 28 members' territory remains NATO's chief function, it isn't sufficient to "line up soldiers and tanks and military equipment along the borders," as the bloc needs "to address the threat at its roots, and it might be in cyber space," adding that an "enemy might appear everywhere in cyberspace." [13]

A year earlier Rasmussen's predecessor as head of the Western military alliance, the Netherlands' Jaap de Hoop Scheffer, foreshadowed NATO's preparations for its 21st century Strategic Concept, unveiled by former U.S. Secretary of State Madeleine Albright and her self-styled Group of Experts at NATO headquarters this May 17, in stating "we need to take a broader approach and gradually consider the notion of collective security, rather than strictly collective defence." [14]

To expand the North Atlantic bloc's missions internationally, the distinction between military threats and a multitude of self-identified security concerns needs to be blurred.

The litany of non-military excuses for NATO interventions throughout the world includes frequently intangible, unverifiable and highly subjective factors like perceived missile threats, climate change, demographic shifts and dislocations, and "storms and floodings" amid "a myriad of determined and deadly threats" as Lord Peter Levene, chairman of Lloyd's of London, characterized NATO's current challenges at a conference his firm co-organized with the military bloc last October 1. [15]

Arguably by their very nature, cyber security issues are among the most amorphous, nebulous and ethereal threats that can be devised (and concocted) and as such are characterized by near universal applicability and the effective impossibility of being disproven. An indispensable arrow in the Pentagon's and NATO's collective quiver, then.

In the speech cited above, former NATO chief Jaap de Hoop Scheffer specifically addressed the matter of cyber security, demanding that NATO "should consider drawing on the unique capabilities that already exist in our military and look to build on them. They could, for example, form a rapid response service to support Allies and perhaps even partners in the event of an attack. And given the vital role that space and satellites now play within our cyber networks, should we not also start to follow activities in space more closely and consider the implications for our security?" [16]

In June of last year U.S. ambassador to NATO Ivo Daalder, former National Security Council staffer currently on loan from the Brookings Institution, also tested the waters on whether the Alliance's Article 5 war clause should be activated in response to "energy strangulation" or "a cyber or bio attack of unknown origin." [17]

“Energy strangulation” – that is, the accusation of energy cutoffs to Europe – is inevitably coupled with charges of cyber attacks in Europe and both are in exclusive reference to Russia. For example, in Scheffer’s recommendation of last year on the application of NATO’s Article 5 for cyber and space use he added this:

> “The disruption of a country’s energy supply can destroy the economic and social fabric of a country in a way that resembles a war – yet without a single shot being fired. It is therefore vital that NATO defines what added value it can bring, for example in terms of protecting critical infrastructure or securing chokepoints through which supply lines run.” [18]

In her May 17 remarks to NATO’s North Atlantic Council on the new Strategic Concept, Madeleine Albright stated that “NATO must maintain a flexible mix of military capabilities, including conventional, nuclear, and missile defense” and laid stress on “the primacy of Article 5,” which stipulates that “the Alliance must continue to treat collective defense as its core purpose.”

Among threats justifying the activation of Article 5 are “cyber assaults and attacks on energy infrastructure and supply lines.” [19] Her group’s report demands that NATO “accelerate efforts to respond to the danger of cyber-attacks by protecting its own communications and command systems, helping allies to improve their ability to prevent and recover from attacks, and developing an array of cyber-defense capabilities aimed at effective detection and deterrence.” [20]

Anticipating the Pentagon’s William Lynn by two months, NATO’s Director of Policy Planning Jamie Shea said that “120 countries currently have or are developing offensive cyber attack capabilities, which is now viewed as the fifth dimension of warfare after space, sea, land and air…”

On March 22 “Shea said there are people in the strategic community who say cyber attacks now will serve the same role in initiating hostilities as air campaigns played in the 20th century.” [21]

Shortly after this year’s presidential election in Ukraine, the country became the first non-NATO member to be recruited for cyber defense cooperation with the North Atlantic military bloc. “On 11-12 February 2010, cyber defence experts from Ukraine, NATO and Allied countries participated in the first NATO-Ukraine Expert Staff Talks on Cyber Defence in Kyiv.” [22]

NATO’s pioneer project in this area, though, remains its cyber warfare center in Estonia. The operation’s experts “second-guess potential adversaries, gazing into what they dub the ‘fifth battlespace’, after land, sea, air and space.”

Colonel Ilmar Tamm, the top Estonian military official at the site, was quoted late last month claiming “Definitely from the cyber-space perspective, I think we’ve gone further than we imagined in science fiction.” [23]

Estonian Defence Minister Jaak Aaviksoo spoke with Agence France-Presse about events in 2007 and the present, saying “It clearly heralded the beginning of a new era… It had all the characteristics of cyber-crime growing into a national security threat. It was a qualitative change, and that clicked in very many heads. Cyber-security, cyber-defence and cyberoffence are here to stay. This is a fact of life.” [24]

On April 23, the second day of a NATO foreign ministers meeting in the Estonian capital, a memorandum of understanding was signed which “creates a legal framework for cyber defence cooperation between NATO and Estonia. It will facilitate the exchange of information and provide means for create a mechanism for assistance in case of cyber attacks.

> “The agreement was signed on behalf of NATO by Amb. Claudio Bisogniero, Deputy Secretary General…” [25]

The individual who personifies the organic and inextricable connection between the Pentagon and NATO is the one who simultaneously heads up U.S. European Command and is NATO’s Supreme Allied Commander Europe, from General Dwight Eisenhower in 1951 to Admiral James Stavridis currently.

On February 2 of this year Stavridis said that because of “attacks on computer networks in Estonia, Georgia, Latvia and Lithuania in the past several years,” although he didn’t offer either specifics on or substantiation for the claim, “the definition of protections for NATO members should be expanded.”

The four countries identified as victims leave no doubt as to who Stavridis views as the perpetrator.

Addressing an Armed Forces Communications and Electronics Association conference and speaking of NATO’s Article 5, he said that the “likelihood that the next conflict will start with a cyber attack rather than a physical attack highlights the importance of changing the treaty’s definitions.” [26]

Employing a line of reasoning that he has repeated in the interim, he said: “In NATO we need to talk about what defines an attack. In a country like Estonia, Latvia, Lithuania, all NATO members, what defines an attack? I believe it is more likely that an attack will come not off a bomb rack on an aircraft, but as electrons moving down a fiber optic cable. So this is a very real and germane part of this challenge that we face in the cyber war.”

NATO’s top military commander was also paraphrased as saying that “NATO has taken the first step toward making cyber warfare combat an international effort by standing up the Cooperative Cyber Defence Center of Excellence in 2008 in Estonia, but facing cyber threats will require cooperation among U.S. government agencies, and between governments and industry as well.” [27]

In early May Stavridis delivered a speech in Paris in which he again highlighted “new threats facing NATO from cyber space” in relation to “NATO’s role in combating these threats, in particular Article 5 operations and collective defence.” [28]

On May 19 he appeared as the guest of honor at a special Commanders Series event at the Atlantic Council [29] in Washington, D.C., where he was introduced by Madeleine Albright two days after she had presented her Group of Experts report on NATO’s 21st century global Strategic Concept in Brussels.

Stavridis boasted that NATO nations have a combined gross domestic product of $31 trillion, have over two million men and women under arms, and "130,000 soldiers and sailors and airmen and Marines on missions on three different continents." The above despite the fact that "No nation has ever attacked a NATO nation." [30]

His presentation was accompanied by slides and his comments included: "I think that Secretary Albright's paper hits this exactly right. We must, as an alliance, begin to think coherently about cyber. We find here the flags of four states that have been involved in cyber intrusions. [Presumably the four former Soviet states he identified in February.] I think it's important that as an alliance, we begin to come to grips with what is a cyber attack.

> "We need centers that can focus on it; we need procedures to provide defensive means in this world of cyber." [31]

Cyber defense and its inevitable correlate, cyber warfare, are integral components of Pentagon and NATO warfighting doctrine, embodied as such in the U.S.'s new Quadrennial Defense Review and in NATO's latest Strategic Concept to be formally adopted at the bloc's summit in Lisbon, Portugal this November.

Cyber warfare as an element of military operations in the other four spheres – land, air, sea and space, especially in the last – and in its own right. With the most advanced computer networks in the world and the most capable corps of cyber specialists in all realms, the world's military superpower has launched the first military cyber command.

Notes

1) Agence France-Presse, May 12, 2010
2) Associated Press, May 5, 2009
3) U.S. Department of Defense, May 21, 2010
4) Financial Times, January 31, 2010
5) U.S. Strategic Command
http://www.stratcom.mil/about
6) Stars and Stripes, May 22, 2010
7) Air Force Times, February 19, 2010
8) Stars and Stripes, May 22, 2010
9) Air Force Times, May 19, 2010
10) Agence France-Presse, May 12, 2010
11) Wall Street Journal, August 26, 2008
12) The Telegraph, March 18, 2010
13) Agence France-Presse, March 4, 2010
14) North Atlantic Treaty Organization, March 11, 2009
15) Thousand Deadly Threats: Third Millennium NATO, Western Businesses Collude
On New Global Doctrine
Stop NATO, October 2, 2009
http://rickrozoff.wordpress.com/2009/10/02/thousand-deadly-threats-third-millennium-nato-western-businesses-collude-on-new-global-doctrine
16) North Atlantic Treaty Organization, March 11, 2009
17) Defense News, June 8, 2009
18) North Atlantic Treaty Organization, March 11, 2009
19) North Atlantic Treaty Organization, May 17, 2010
20) Aviation Week, May 18, 2010

21) Defense News, March 23, 2010
22) North Atlantic Treaty Organization, February 22, 2010
23) Agence France-Presse, April 24, 2010
24) Ibid
25) North Atlantic Treaty Organization, April 23, 2010
26) Defense News, February 2, 2010
27) Ibid
28) North Atlantic Treaty Organization
Supreme Headquarters Allied Powers Europe
May 7, 2010
29) Atlantic Council: Securing The 21st Century For NATO
Stop NATO, April 30, 2010
http://rickrozoff.wordpress.com/2010/05/01/atlantic-council-securing-the-21st-century-for-nato
30) Atlantic Council, May 19, 2010
31) Ibid

The original source of this article is Stop NATO

Articles by: Rick Rozoff

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca