GlobalResearch
Center for Research on Globalization

Pentagon Partners With NATO To Create Global Cyber Warfare System

By Rick Rozoff
Global Research, October 09, 2010
Stop NATO 8 October 2010

Region: USA
Theme: US NATO War Agenda

U.S. Cyber Command is scheduled to be activated this month, in the words of a Reuters dispatch "ready to go to war in cyberspace" with full operational capability.

The launching of the world's first multi-service – with the involvement of all major branches of the U.S. armed forces: Air Force, Army, Marine Corps and Navy – military command is being coordinated with a complementary initiative by the North Atlantic Treaty Organization in Europe, the joint effort striving toward a worldwide cyber warfare system.

Last month the U.S. Defense Department's Joint Task Force Global Network Operations command was deactivated and absorbed into U.S. Cyber Command (CYBERCOM) after a decade-long existence.

In describing the transition, the Pentagon's press service recounted that the task force had worked on "the best ways to operate on the cyber battlefield" with "a dual mission to conduct offensive and defensive cyber operations." In 2003 it was assigned to U.S. Strategic Command (STRATCOM), under whose sponsorship CYBERCOM is also being inaugurated. The next year Joint Task Force Global Network Operations was reconfigured "to assume the offensive role" of the above-mentioned shield-and-sword function.

Air Force General Kevin Chilton, the commander of U.S. Strategic Command, presided over the September 7 turnover ceremony. Army Lieutenant General Carroll Pollett, head of the Task Force Global Network Operations since 2008, is now reduced to remaining director of the Defense Information Systems Agency, at whose Arlington, Virginia site the ceremony was held, though the Pentagon's Defense Information Systems Agency is slated to follow CYBERCOM to Fort Meade, Maryland.

General Pollett's comments at the event included: "(Information) has become an operational imperative in our ability to deliver decisive capabilities to warfighters and our national leaders.

> "Cyberspace has evolved into a new warfighter domain.
>
> "Cyberspace has proven equal and just as important as air, sea, land and space as a domain. It's clear that it must be defended and operationalized." [1]

His characterization of cyber space as the fifth military domain is consistent with the standard use of that trope by Pentagon officials, a variant of which is fifth battlespace. [2] When the leaders of the mightiest military in the history of the world discuss adding a new

dimension to the traditional ones of infantry, air force, navy, marine, and satellite and missile operations, they are planning not only for an extension of warfare preparations to a new realm but into one which is related to and in many ways dominates the others.

The first commander of CYBERCOM, General Keith Alexander, said two weeks after his appointment and CYBERCOM's launching on May 21 that the Pentagon "depends on its networks for command and control, communications, intelligence, operations and logistics" and that the mission of his command is to "deter, detect and defend against emerging threats against our nation in cyberspace."

The general, who is simultaneously head of the Defense Department's National Security Agency, also said that "clear rules of engagement" need to be defined for cyber warfare and that "We have to look at it in two different venues – what we're doing in peacetime and in wartime." [3]

In his first public comments since assuming his new command, Alexander was already speaking of its role within a war context.

A few days before, Strategic Command chief Chilton and Deputy Secretary of Defense William Lynn also asserted that CYBERCOM's next priority is "to develop the rules of engagement of cyber warfare." [4]

On the rare occasions when the Pentagon's establishing an unprecedented military command for cyber operations is mentioned in the news media at all, the preferred word in defining its purpose is defense. When military and Defense Department personnel speak among themselves more direct terms are employed: Warfare, warfighting, wartime, rules of engagement, battlefield, battlespace.

Regarding Washington's use of the word defense in general, when the U.S. changed the name of the Department of War to the Department of Defense in 1949 it achieved one thing: The name was changed. A year later the Defense Department was embroiled in the Korean War.

The American military has not been used to defend the U.S. mainland since 1812, when the United States instigated a war with Britain by invading Canada. It has not been used even to defend American territories since the less-than-effective defense of Pearl Harbor in 1941 (Hawaii did not become a state until 18 years later) and ensuing fighting in even more remote island possessions: The Philippines, Guam, Wake Island and the Midway Atoll.

During the U.S.'s first war in Europe, initially in France and later in Soviet Russia from 1917-1919, Washington called its armed forces what they were. Expeditionary.

In the war waged by the U.S. and NATO against Yugoslavia in 1999 and in the invasion of Iraq four years later the two countries' power, broadcasting and telecommunications networks were targeted for disabling and destruction. In the case of Yugoslavia graphite bombs were used to shut down the nation's electrical power grid.

Recent rumors that the Stuxnet computer virus was used to attack Iran's civilian nuclear power plant at Bushehr provide an example of how the capabilities CYBERCOM is developing for its offensive, its wartime, contingencies could be employed. In a world increasingly dependent on information technology, cruise missiles and graphite bombs have been superseded by cyber attacks.

In addition to the Pentagon's Prompt Global Strike project [5] for launching intercontinental ballistic and hypersonic cruise missile strikes anywhere in the world within 60 minutes, with the interval to shrink to a fraction of that time in the future, and with the development of super stealthy strategic bombers able to evade radar and air defenses and penetrate deep into the interior of targeted countries, a global cyber warfare capability would render the world defenseless in the face of American blackmail. And attacks. The foreign equivalents of the Pentagon's Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) system could be neutralized.

Not only would Iran be vulnerable, but Russia and China as well.

The September-October edition of Foreign Affairs, the journal of the Council on Foreign Relations, contains an article by Deputy Secretary of Defense William Lynn called "Defending a New Domain: The Pentagon's Cyberstrategy" in which he announced that "the Pentagon has built layered and robust defenses around military networks and inaugurated the new U.S. Cyber Command to integrate cyberdefense operations across the military," [6] and where he spelled out the five components of the Pentagon's cyber warfare strategy:

– Cyber must be recognized as a warfare domain equal to land, sea, and air;

– Any defensive posture must go beyond "good hygiene" to include sophisticated and accurate operations that allow rapid response;

– Cyber defenses must reach beyond the department's dot-mil world into commercial networks, as governed by Homeland Security;

– Cyber defenses must be pursued with international allies for an effective "shared warning" of threats; and

– The Defense Department must help to maintain and leverage U.S. technological dominance and improve the acquisitions process to keep up with the speed and agility of the information technology industry. [7]

The Defense Department is due to release a cyber strategy document this autumn, synchronized with the full operationalization of CYBERCOM and ahead of the NATO summit in Portugal on November 19-20.

On August 28 the Washington Post ran a feature entitled "Pentagon considers preemptive strikes as part of cyber-defense strategy" which detailed the following:

The Defense Department is working on "an aggressive approach" to cyber operations which "includes preemptive actions such as knocking out parts of an adversary's computer network overseas."

According to Pentagon budget documents, it is developing a full range of weapons capabilities to permit "attack and exploitation of adversary information systems" that will "deceive, deny, disrupt, degrade and destroy" information and information systems.

The deployment of software and hardware tools for the above purposes is "the next logical step in a cyber strategy outlined last week by Deputy Secretary of Defense William J. Lynn III," one of so-called "active defense." [8]

In August CYBERCOM chief General Keith Alexander spoke at the LandWarNet 2010 conference in Tampa, Florida whose theme was Providing Global Cyber Dominance to Joint/Combined Commanders. He reiterated the contention that "cyberspace is now a domain alongside air, land, sea, and space." [9] More ominously, he added: "We have to have offensive capabilities, to, in real time, shut down somebody trying to attack us." [10]

For "active defense" read the capacity to launch preemptive attacks not only on individual hackers but on entire national computer networks.

The Washington Post cited an unnamed senior Pentagon official arguing the same point: "I think we understand that in order for us to ensure integrity within the military networks, we've got to be able to reach out as far as we can – once we know where the threat is coming from – and try to eliminate that threat where we can." Even though "taking action against an attacker's computer in another country may well violate a country's sovereignty." [11]

A reporter from the newspaper warned that "The Pentagon has standing rules of engagement for network defense, such as the right of self-defense. But the line between self-defense and offensive action can be difficult to discern." [12]

Reactions to the above statements and others like them have emanated from Russia and China, if not from official sources. A Russian website posted an analysis last month under the title "US gets ready to knock the world offline" which stated that "After October 1 [the original date for activating CYBERCOM as an independent command] thousands of US military hackers and spies will get down to their cyber war activities." [13]

The author reminded his readers that in April of this year Central Intelligence Agency Director Leon Panetta unveiled the CIA 2015 blueprint for the next five years, the "second pillar" of which includes "investing in technology to extend the CIA's operational and analytic reach and becom[ing] more efficient. Agency personnel must be able to operate effectively and securely in a rapidly changing global information environment. The plan boosts the CIA's potential for human-enabled technical collection and provides advanced software tools…." [14]

In May, the same month CYBERCOM was activated, the White House approved this year's Cyberspace Policy Review.

The Russian source also said that "Numerous publications in the US mass media show that the reform of the national cyber defense forces as well as the introduction of the doctrine and strategy of cyber war are soon to be completed. As for the US cyber strategy, we can assume that it is in line with the general concept of US global leadership." [15]

A few weeks ago an article appeared in the Global Times by a researcher at the Development Research Center of the State Council of China who wrote, "To control the world by controlling the Internet has been a dominant strategy of the US" and "the national information security strategy of the US has evolved from a preventative strategy to a preemptive one."

> "The ultimate goal is for the US to [have] the ability to open and shut parts of the Internet at will."

The article claims that in 2004 the U.S. shut down the "ly" domain name and cut off all Internet services in Libya and "In May 2009, Microsoft announced on its website that they would turn off the Windows Live Messenger service for Cuba, Syria, Iran, Sudan and North Korea, in accordance with US legislation." [16]

The Washington Post story quoted from earlier added that the Pentagon's disabling of a Saudi website in 2008 "also inadvertently disrupted more than 300 servers in Saudi Arabia, Germany and Texas." [17]

The Chinese author further asserted that "the five core areas of Internet infrastructure are monopolized by US":

– IT giants, including high-performance computers, operating systems, database technologies, network switching technologies and information resource libraries.

– Across the world, around 92.3 percent of personal computers and 80.4 percent of super computers use Intel chips, while 91.8 percent of personal computers use Microsoft operating systems, and 98 percent of core server technology lies in the hands of IBM and Hewlett-Packard.

– Meanwhile, 89.7 percent of database software is controlled by Oracle and Microsoft, and 93.5 percent of core patented network switching technology is held by US companies.

– After the control of Internet infrastructure and hardware and software systems, the US is now turning to Internet content.

– The US government has adopted macro-control and focus-funding to actively use IT giants to create a global Internet infrastructure which could be manipulated by the US. [18]

He also mentioned that Senator Joseph Lieberman, chairman of the Senate Committee on Homeland Security and Governmental Affairs, recently presented to his colleagues in the Senate a bill called Protecting Cyberspace as a National Asset which provides for the president to "order Google, Yahoo and other search engine operators to suspend Internet services.

> "And other US-based Internet service providers could also be under the control of the president when 'Internet security emergencies' occur.
>
> "If so, the US president would officially have the power to open or close the Internet." [19]

The Chinese expert's apprehensions were confirmed by retired Air Force general Michael Hayden – director of the National Security Agency from 1999-2005, principal deputy director of National Intelligence from 2005–2006 and director of the CIA from 2006-2009 – who last month stated, as paraphrased by Reuters, that "Cyberterrorism is such a threat that the U.S. president should have the authority to shut down the Internet in the event of an attack." In his own words: "My personal view is that it is probably wise to legislate some authority to the President, to take emergency measures…when he feels as if he has to take these measures" [20]

The Pentagon and the White do not intend to act alone in developing an international cyber

warfare structure.

U.S. cyber warfare security experts met in Omaha, Nebraska shortly after CYBERCOM was inaugurated in May for a two-day Strategic Command Cyberspace Symposium which included “cyber commanders from several U.S. combatant commands, NATO, Japan and the U.K.” [21]

In the same month, May, the NATO Group of Experts headed by former U.S. Secretary of State Madeleine Albright released its report, NATO 2010, which stated “NATO should plan to mount a fully adequate array of cyber defence capabilities, including passive and active elements.” [22]

A feature three weeks later in the Sunday Times of London disclosed that “A report by Albright’s group said that a cyber attack on the critical infrastructure of a Nato country could equate to an armed attack, justifying retaliation.

> “‘A large-scale attack on Nato’s command and control systems or energy grids could possibly lead to collective defence measures under article 5,’ the experts said.”

The article also cited a legal expert at NATO’s Cooperative Cyber Defence Centre of Excellence established in Estonia in 2008 affirming that “because the effect of a cyber attack can be similar to an armed assault, there is no need to redraft existing treaties.” That is, the Alliance’s Article 4 – used to move Patriot anti-ballistic missiles into Turkey on the eve of the war against Iraq in 2003 – and its Article 5 – used for NATO’s participation in the war in Afghanistan – can be evoked and activated in the event of a cyber attack.

The Sunday Times piece added:

> “[NATO] concerns follow warnings from intelligence services across Europe that computer-launched attacks from Russia and China are a mounting threat.
>
> “NATO is considering the use of military force against enemies who launch cyber attacks on its member states.
>
> “The move follows a series of Russian-linked hacking against Nato members and warnings from intelligence services of the growing threat from China.” [23]

The preceding month the 13th NATO Cyber Defence Workshop was held in the Estonian capital of Tallinn. Speaking to the attendees, Defence Minister Jaak Aaviksoo said, “The robust national cyber security systems of Allies will be building blocks of a convincing NATO cyber defence capability.” [24]

In June a four-day international conference “tackling the issue of cyber conflicts” was held at the NATO center in Estonia, which borders Russia. A keynote address was delivered by Melissa Hathaway, Cybersecurity Chief at the U.S. National Security Council.

Gloria Craig, Director for International Security Policy at Britain’s Ministry of Defence, insisted on the urgency of expanded cyber warfare capacities, stating “As of now NATO is not prepared for a global cyberattack.” [25]

Also in June, over "100 participants from leading global IT companies, the banking sector, the intelligence community, NATO, the EU and other institutions" attended the Cyber Defence in the Context of the New NATO Strategic Concept conference in Romania, which issued a report advocating that "NATO must 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 defence capabilities…." [26]

In August NATO revealed that it has created a new Emerging Security Challenges Division "in order to deal with a growing range of non-traditional risks and challenges," including cyber operations. "The Emerging Security Challenges Division brings together various strands of expertise already existent in different parts of NATO Headquarters. Merging this work into one Division will give it greater focus and visibility." [27]

This month NATO's Consultation, Command and Control Agency (NC3A) organized a conference in the Czech Republic, and the Alliance's advanced technologies procurement agency announced that "NATO is looking at beginning to invest up to 930 million euros ($1.3 billion) in 2011 and 2012 in multi-year projects to address key security challenges, such as cyber defence, support to NATO's Afghanistan effort and maritime security." [28]

A recent report divulged that in an interview with the Suddeutsche Zeitung NATO Secretary General Anders Fogh Rasmussen said he wants the Alliance to "extend the definition of attacks which trigger activation of the alliance to include cyber attacks" [30] as part of the new Strategic Concept to be endorsed at its summit next month.

In mid-September the Pentagon's second-in-command, William Lynn, was in Brussels to address the North Atlantic Council, NATO's highest governing body, as well as a defense-related think tank. [29]

Rallying Washington's military allies ahead of the summit in November, he said: "NATO has a nuclear shield, it is building a stronger and stronger [missile] defence shield, it needs a cyber shield as well….The Cold War concepts of shared warning apply in the 21st century to cyber security. Just as our air defences, our missile defences have been linked so too do our cyber defences need to be linked as well." [31]

As Lynn arrived in Brussels U.S. European Command was finishing the 15-day Combined Endeavor 2010 exercise, "the world's largest military communications and information systems exercise," at the Joint Multinational Simulations Center at the Grafenwoehr Training Area in Germany, Altogether there were 1,400 participants from 40 countries:

The U.S., Germany, Austria, Afghanistan, Armenia, Albania, Azerbaijan, Bulgaria, Bosnia, Britain, Canada, Croatia, the Czech Republic, Denmark, Estonia, France, Finland, Germany, Georgia, Hungary, Italy, Iraq, Ireland, Kazakhstan, Lithuania, Macedonia, Moldova, Montenegro, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Switzerland, Spain, Serbia, Turkey and Ukraine.

A U.S. European Command spokesman said of the event: "There's an 'endeavor' now in the Pacific, Pacific Endeavor. There is one in North America that uses South America and Canada to interconnect their network communication systems. This exercise that we do here in Grafenwoehr has branched-out world-wide, and every major command is launching their version of it." [32]

Since 2006 the U.S. has also led Africa Endeavor military exercises on the continent, "Africa's largest communications interoperability exercise," [33] first under U.S. European Command and recently under the new U.S. Africa Command. Africa Endeavor 2010 was held in Ghana in August with the participation of 36 African nations.

Worldwide is the correct word for the military network the Pentagon has built in recent years, as is evidenced by the nations participating under U.S. command in Combined Endeavor 2010 and Africa Endeavor 2010: 75 countries with Afghanistan and Iraq among them.

American-led multinational training exercises and war games on the same scale are routinely held throughout Europe, at the moment this year's second Joint Warrior exercise – Europe's largest war games – in, off the coast and over the skies of Scotland with 30 countries, 10,000 troops, 30 warships, three submarines and 21 air and helicopter units. Military maneuvers of comparable size occurred during the summer in the Asia-Pacific region when the U.S. led this year's 14-nation Rim of the Pacific war games, the world's largest multinational maritime exercise, with an estimated 22,000 troops, 34 ships, five submarines and over 100 aircraft involved. [34]

Last month's Combined Endeavor exercise in Germany included a cyber defense component for the first time. Participants from 26 countries and two organizations, NATO and the Cooperative Cyber Defence Centre of Excellence based in Estonia, engaged in planning for cyber operations at the Joint Multinational Simulations Center in Grafenwoehr from September 3-15.

Since the end of the Cold War, and especially in the past decade, the Pentagon has expanded its activities – bombing campaigns, wars, invasions, multinational maneuvers and war games, base building and takeovers, troop and missile shield deployments, training programs, establishing military transport networks – throughout the world.

Through the eastward expansion of NATO, the world's only military bloc, and the launching of U.S. Africa Command two years ago, the U.S. has gained military dominance over two entire continents.

It has military partnerships with almost every nation in Europe, Africa, the Middle East and Asia, and has acquired new bases and other military facilities in Eastern Europe, Africa, the Middle East, Asia, the South Pacific and South America: Kosovo, Bulgaria, Romania, Hungary, Poland, Djibouti, Seychelles, Iraq, Israel, Kuwait, Afghanistan, Kyrgyzstan, Australia and Colombia.

Washington has increased its military presence in several continents to achieve its 21st century geopolitical objectives. To control access to and the transport of hydrocarbon resources, the Pentagon has expanded its role in the Persian Gulf, Africa's Gulf of Guinea, the Black Sea and in nations near the Caspian Sea Basin. With the reactivation of the U.S. Fourth Fleet in 2008, the U.S. is positioned to dominate the Caribbean Basin, including Colombia, Venezuela and Panama on its southern shores.

The U.S. is putting the pieces in place for a global interceptor missile system with the deployment, directly and with partners, of Patriot Advanced Capability-3, Standard Missile-3, Terminal High Altitude Area Defense, X-Band Radar and other missile shield components to Poland, Israel, Bahrain, Kuwait, Qatar, the United Arab Emirates, Japan, South Korea and

Australia, with the Black Sea, the Mediterranean Sea, Baltic Sea and South Caucasus as planned future sites.

The Pentagon will be satisfied with nothing less than full spectrum dominance throughout the world – and above the world. It is now adding to its military superiority in the realms of land, air, sea and space control of the fifth battleground: Cyberspace.

Notes

1) American Forces Press Service, September 8, 2010
2) U.S. Cyber Command: Waging War In World's Fifth Battlespace
Stop NATO, May 26, 2010

http://rickrozoff.wordpress.com/2010/05/26/u-s-cyber-command-waging-war-in-worlds-fifth-battlespace

3) Agence France-Presse, June 4, 2010
4) Stars and Stripes, June 2, 2010
5) Prompt Global Strike: World Military Superiority Without Nuclear Weapons
Stop NATO, April 10, 2010

http://rickrozoff.wordpress.com/2010/04/10/prompt-global-strike-world-military-superiority-without-nuclear-weapons

6) William J. Lynn III, Defending a New Domain:The Pentagon's Cyberstrategy
Foreign Affairs, September/October 2010

http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

7) U.S. Department of Defense, August 25, 2010

http://www.defense.gov/news/newsarticle.aspx?id=60600

8) Ellen Nakashima, Pentagon considers preemptive strikes as part of cyber-defense strategy
Washington Post, August 28, 2010

http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849.html

9) United States Army, August 4, 2010
10) Army News Service, August 3, 2010
11) Washington Post, August 28, 2010
12) Ibid
13) Leonid Savin, US gets ready to knock the world offline
Strategic Culture Foundation, September 6, 2010

http://www.strategic-culture.org/news/2010/09/06/us-gets-ready-to-knock-the-world-offline.html

14) Central Intelligence Agency, April 26, 2010

15) Strategic Culture Foundation, September 6, 2010
16) Chen Baoguo, US controls threaten Internet freedom
Global Times, August 24, 2010

http://opinion.globaltimes.cn/commentary/2010-08/566394.html

17) Washington Post, August 28, 2010
18) Global Times, August 24, 2010
19) Ibid
20) Reuters, September 26, 2010
21) Stars and Stripes, June 2, 2010
22) North Atlantic Treaty Organization

http://www.nato.int/strategic-concept/expertsreport.pdf

23) Sunday Times, June 6, 2010
24) North Atlantic Treaty Organization, June 3, 2010
25) Agence France-Presse, June 9, 2010
26) North Atlantic Treaty Organization, June 7, 2010
27) Defence Professionals (Germany), August 4, 2010
28) Reuters, October 7, 2010
29) NATO Provides Pentagon Nuclear, Missile And Cyber Shields Over Europe
Stop NATO, September 22, 2010

http://rickrozoff.wordpress.com/2010/09/22/2463

30) The H Security, October 1, 2010
31) Agence France-Press, September 15, 2010
32) United States European Command, September 8, 2010
33) U.S. Africa Command, January 12, 2010
34) Asia: Pentagon Revives And Expands Cold War Military Blocs
Stop NATO, September 14, 2010

http://rickrozoff.wordpress.com/2010/09/15/asia-pentagon-revives-and-expands-cold-war-military-blocs

---