AARMS
Vol. 11, No. 1 (2012) 13–26

SECURITY

The geostrategic struggle in cyberspace between the United States, China, and Russia

VIKTOR NAGY

National University of Public Service, Budapest, Hungary

Since the early 2000s, geopolitics has been affected by a new domain of human activity cyberspace. In this study we argue that cyber power, constituted by national information technology capabilities, supplements both geopolitical land power and sea power, and has a role equally important as other domains (land, sea, air, and space) in modern military conflict between peer opponents. By this, we intend to prove that the effective use of cyber power is indispensable in the geopolitical struggle between great powers. This struggle is and has always been characterized by the struggle for space. As cyberspace has become an important area for human activity, a nation cannot avoid trying to control and, when necessary, fight for this new, artificial space. Also, the effective control of cyberspace underpins a nation's control of other spaces. The main holders of international cyber power are the United States, China, and Russia. China and Russia originally started to create their Information Operations capabilities to take advantage of Western vulnerabilities. However, subsequent Chinese and Russian development in the IT sector caused them to be sufficiently vulnerable to loose their asymmetrical advantage in Information Operations and to turn it to a conventional means in the struggle between great powers.

Introduction – Geostrategy in cyberspace, cyber power

At the turn of the 19th and 20th centuries, advocates of geopolitics then the newest subfield of international relations began to argue that human communities tend to be affected by their surroundings, i.e. the geography of the peace of land they inhabit. Culture, economy, politics, military strategy etc. are ultimately all formed by geography and by other groups of people whose actions are formed by their own geographies. At the beginning of the second decade of the 21st century, nations and international institutions formed by nations are the prime subjects of geopolitics.[i] Geostrategy – the

[i] Some authors argue that multinational corporations (MNC) are actors in international relations in their own right. Although they ceratainly play an important role, most of MNCs are only multinational in their operations, but not in leadership. As such, we regard them as tools in geopolitics and geostrategy.

Received: August 24, 2011

Address for correspondence:
VIKTOR NAGY
E-mail: nagy.viktor@kfh.hu

practical realization of geopolitics – is the foundation of national behaviors in the space nations live and surrounded by.

During the course of history, a political entity's total power consisted of land power and sea power. Land power is supported by the sheer landmass, the natural resources and the size of the population a nation possesses assets that enable a nation to build land armies. Sea power is based on navigable harbors, commerce, and the economic and technological foundations to build a navy. Thus, military land and sea (naval) power supports geopolitical national land and sea power, while military air and space power supports both.

We argue that by now, "*a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures*",[ii] known as cyberspace, has evolved enough to significantly affect geostrategy. The information revolution that has created new space – a new domain – of human activity is mostly over. National and military presence in cyberspace has become vital to maintain presence in all other domains, putting its importance in supporting land and sea powers on par with air and space power. The ubiquitous nature of cyberspace – the fact that it has become essential to any sort of power projection – translates to the fact that cyberspace is now vital for maintaining national power at its entirety and thus for national security. As such, it is now at the forefront of the geostrategic struggle – ultimately, the struggle for space – between great powers, most notably of the United States of America, China, and Russia. These three countries constitute and possess the better part of worldwide cyber power, or "the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power".[1]

The most contested domain: cyberspace

The fact that cyberspace is man-made does not alter the fact that nation-states behave in it just as they do in other domains, since activity in the "virtual world" produces very real effects. Similarly to the advent of human activity in the other domains, cyberspace is now strongly contested. Cyberspace has by now been built, but even the definition of its inner boundaries is yet to be defined, and then set. Until then, the struggle between all interested parties to invade as much of its territory as possible is on.[iii] This is a

[ii] Definition by the 2006 National Military Strategy for Cyberspace Operations by the Joint Chiefs of Staff of the armed forces of the United States of America.
[iii] Interview with Marc Watin-Augouard,, inspector general of the French Armed Forces-Gendarmerie, French Ministry of Defense (October 2010).

process that is not unlike the unfolding struggle for the division of the Arctic, the other "no man's land" of our times.[iv] Both include effort to create *opinio juris*[v] by building and showing real capabilities and articulation of national intent to own and control the desired "real estate".

Many refer to cyberspace as a new "global common" at its entirety. Global commons are considered to be out of the jurisdiction of any state, international organization, company, or person, and to be fundamental in supporting human existence. The oceans, the atmosphere, space, and lately cyberspace are typically listed as part of the global commons, *constituting the fabric or connective tissue of the international system*.[2] Though the greater part of cyberspace is truly "common", but as in other domains, some parts of it are already owned by a varying mix of entities: states, international organization, companies, and people. It is those parts of cyberspace that are the property of some entity where great power struggle in cyberspace mostly takes place, while the intention of all concerned parties is to bring as big a chunk of the "common" segments under their ownership as possible.

Information societies and cyber power

Because of its *ability* to render long-established positions in other domains irrelevant, and the chance to operate with only the slightest risk of detection, cyberspace is now – paradoxically and, we think, *temporarily – at the centre of global geostrategic struggle*. After realizing how vulnerable Western power was to information technologies (IT), China and Russia have built up their cyber powers artificially as an asymmetrical tool against the hegemonic position in other domains of the West in general and the United States in particular. Advanced Western societies are highly penetrated by information technology. The widespread advancement of IT in increasing areas of the economy, society, politics, and the military made these national sub-systems far more effective. However, at the same time IT has become a nationwide dependency and vulnerability of Western states. China and Russia came to use these dependencies, and for a time they

[iv] Various ecological, security and military analyses state that due to global warming the now frozen Arctic territories will in the coming decades be navigable and its hidden natural resources will be extractable. As a result of the changing geographical conditions, all neighboring states intend to claim as much sovereign territory as possible and all trading powers are trying to secure its free navigability. Part of the neighboring states' strategy is to show off their capability to operate in the Arctic, communicate their plans to increase those capabilities, and to underline their intention of possession.

[v] In international law, opinio juris is the subjective element which is used to judge whether the practice of a state is due to a belief that it is legally obliged to do a particular act. When opinio juris exists and is consistent with nearly all state practice, customary international law emerges.

managed to turn their greatest disadvantage – lack of advanced information infrastructure – to an effective weapon and tool against the West. The main focus of this tool is, paradoxically again, catching up with the West in the most advanced technologies, with IT at the centre. But exactly by acquiring advanced technology via *cyber espionage*, China and Russia is by now increasingly sharing the dependency on IT with their Western counterparts, becoming vulnerable themselves both to Western cyber attacks and their own emerging information societies. While China and Russia are still nowhere nearly as advanced as Western nations are, their development deprived cyber power of its asymmetrical nature. Cyber power and struggle in cyberspace can now be considered as part of the *conventional*.

At the same time, out of necessity, Western nations are catching up with turning their cyber power into a geostrategic tool. Exactly the other way around as China and Russia did, the United States and its allies mostly advanced postindustrial countries and technocracies use their broad information society foundations and their high proficiency in IT to build up cyber defenses and then projectable cyber power. Whereas China's and Russia's incentives for building national cyber power was to counterweigh overall Western power and to catch up, the West's is to defend that very power. Besides that, for Western nations creating projectable cyber power, thanks to ample, readily available human and technical resources raw cyber power – is relatively easy.

National cyber power – Cybersecurity and information operations

As stated above, cyber power is vital for national security. National cyber power can be divided into two broad categories: *cybersecurity* and *information operations*. The growing importance of the *critical information infrastructure* – the internet and associated information networks, cell phone networks, banks, e-governance, etc., all part of the international information networks – in supporting and maintaining all *critical infrastructures* – transportation, energy generation and distribution, water distribution, *law enforcement and military*, etc., that are the foundations of the functioning of nations – and the national vulnerabilities it causes constitutes the need for creating national cybersecurity. Cybersecurity is the responsibility of both civilian national security agencies and the military. The focus of cybersecurity is the protection of critical national infrastructure from *cyber attacks* – attacks through the information networks – and the defense of national information infrastructure from both cyber and physical attacks.[3] A secondary but emerging role is the protection of valuable

information from cyber espionage utilizing Computer-Network Operations (CNO).[vi] Because of the ubiquitous and ever-changing nature of cyberspace, it is hard to set boundaries between the responsibilities of civilian and military agencies, creating the need for intense coordination between all actors involved. The military's tasks in cybersecurity are mainly the protection of critical military infrastructure – command centers, military information and communication networks, etc. –, and taking part in the fight against cyber espionage and cyber terrorism where military interests are concerned, and, above all, leading national cybersecurity efforts against wide-scale cyber attacks executed by other governments or militaries. The national cyberspace strategy[4] of the United States of America and the Pentagon's cyber strategy[vii] have established the option for the President to order the military to execute a conventional military counterstrike provided that a cyber attack on the United States has had effects comparable to a military attack. Understanding the international nature of cyberspace, the strategy underlines the importance of international cooperation in cybersecurity.

Information operations (INFOOPS, IO) or information warfare is a set of various technical and human-related subfields within the military reconnaissance and intelligence that are related to using information in fighting the adversary in both the strategic, operational, and tactical levels, combined with the physical destruction of the adversary's information networks. These subfields of INFOOPS are Electronic Warfare (EW), Signal Intelligence (SIGINT), Computer-Network Operations (CNO), Psychological Operations (PSYOPS), Operational Security, and Deception.[5] It is to be noted that all of the military's tasks in national cybersecurity are also part of IO.

The evolution of INFOOPS I. – Estonia and NATO's cybersecurity centre

A modern nation widely utilizing IT is vulnerable to cyber attacks directed at its critical infrastructure. Through such attacks the modern nation-state can be disabled within a very short period of time. The costs of delivering cyber attacks are minimal compared to the costs (financial, human, and the danger of retaliation) of a conventional military attack. Open Source Intelligence (OSINT) methods are perfectly suitable for pre-attack reconnaissance, utilizing information that is readily available. Cyber and physical attacks that can cause the greatest damage at the lowest cost are those against the electronic – including internet-based media, broadcasting, the financial sector, transportation, telecommunication, electricity services, e-government, and the internet

[vi] CNO can be further sub-divided to Computer-Network Attack (CNA), Computer-Network Exploitation (CNE), and Computer-Network Defense (CND).
[vii] Expected to be released in June 2011.

as a whole.[6] After the successful combined attack of these sectors, a nation's economy and its ability to communicate at the national and international levels including the ability to command the military forces can be crippled. It is to be noted, that even though criminal gangs have substantial cyber resources, such a large-scale attack requires the capabilities of a national government.

An attack similar to what is described above was directed against Estonia beginning 26th April 2007. Hundreds of thousands of computers organized into botnets[viii] conducted distributed denial of service (DDOS)[ix] attacks for several weeks against Estonian banks, companies, and media. Estonia accuses Russia with delivering the attack, though the Russian government's involvement was never proven. The reason behind the attack is the relocation of a Soviet war memorial from the inner city of Tallin. The attack was *the first large-scale cyber attack against a country's critical information infrastructure*, and highlighted the vulnerabilities of modern information societies.

As a response to the attack, NATO has set up its *Cooperative Cyber Defence Centre of Excellence* (CCD COE)[x] in Tallin. CCD COE focuses on researching and building Alliance-level cybersecurity, making sure that NATO is prepared to defend its Member States and its own institutions against cyber attacks.

The evolution of INFOOPS II. – Georgia and NATO's new Strategic Concept

Cyber attacks can be devastating by themselves, but the greatest effects can be achieved when INFOOPS is integrated with conventional military operations. After taking out the national information infrastructure utilizing botnet-delivered DDOS attacks, the ensuing chaos provides a perfect ground for conventional military strikes or an invasion. By blocking national and international communications, it is hard for both the world and the affected nation to figure out what is going on, and INFOOPS can have the same affect on the adversary's military. A military without command and control and information can not conduct modern warfare, and by the time communication networks are restored it might be already too late. The first such combined attack happened during the Russian military's invasion of Georgia from 7th August 2008. Besides

[viii] A botnet (robot network) is a network of private computers infected with malware and controlled as a group without the owners' knowledge.

[ix] During a DDOS attack, multiple systems flood the bandwidth or resources of a targeted computer system, attempting to make it unavailable to its intended users..

[x] CCD COE was established 14th of May 2008. Sponsoring Nations include Estonia, Latvia, Lithuania, Germany, Hungary, Italy, the Slovak Republic, and Spain. The United States, Turkey and Poland have so far indicated to join. Source: http://www.ccdcoe.org/

mimicking the cyber attack against Estonia, *Russia utilized INFOOPS against another nation for the first time in history*.

The attack alarmed NATO and especially the Member States that are bordering Russia and its neighbors. NATO's new *Strategic Concept*[xi] deals way more extensively with cyber threats compared to its predecessor of 1999. Besides calling for closer cooperation in and greater centralization of cybersecurity, the document hints at collective conventional military retaliation to a cyber attack against a Member State: when referring to Article V of the North Atlantic Treaty, the Concept uses the term "attack" instead of the original term of "armed attack" as a prerequisite of collective defense.

The evolution of INFOOPS III. – Stuxnet, Western cyber power and USCYBERCOM

The latest step in the evolution of cyber attacks was the introduction of malicious software (malware) capable of the direct physical destruction of critical industrial infrastructure. The existence of the *Stuxnet* computer worm[xii] was first reported in June 2010. Stuxnet was designed to attack programmable logic controllers (PLCs) made by the German company Siemens. PLCs control timing-sensitive industrial processes. Such – contraband – PLCs are used in Iranian nuclear facilities. Stuxnet was uploaded to Iranian computer systems via USB-flash drives. As the Georgian Foundation for Strategic and International Studies described Stuxnet's operation, "*when Stuxnet found a targeted PLC, it injected its own code into it, concealing itself and the alterations it made. This caused the PLC to misdirect the controlled process—too fast or too slow; early or late; too much or too little*."[7] Stuxnet's design allows attackers to manipulate industrial equipment without the operators knowing.[xiii] As a result, the installation of the Bushehr nuclear power plant was delayed,[xiv] and the uranium centrifuges of Natanz were partially disabled.[xv]

It is widely suspected that the United States Cyber Command (USCYBERCOM, see below) and Israel's Unit 8200 of the Israeli Intelligence Corps[xvi] are responsible for the creation and deployment of Stuxnet.[xvii] The motive was to slow down the Iranian

[xi] It was approved by the leaders of the Member States 19th November 2010.
[xii] A computer worm is a self-replicating malware computer program akin to a computer virus, but it does not need to attach itself to an existing program.
[xiii] *The Stuxnet Worm*, Symantec briefing, (January 2011).
[xiv] Source: *Stuxnet preventing Iran from opening Bushehr*, The Times of India, (September 2010).
[xv] Source: Iran Confirms Stuxnet Worm Halted Centrifuges, CBS News (November 2010).
[xvi] The unit is responsible for collecting signal intelligence and code decryption.
[xvii] Sources: With Stuxnet, Did The U.S. And Israel Create a New Cyberwar Era? Wired Danger Room (January 2011); Israel seen as prime cyberattack suspect, United Press International (October 2010); 'Stuxnet virus set back Iran's nuclear program by 2 years', Jerusalem Post (December 2010).

nuclear program that would have otherwise only been possible by conventional military strikes. Computer security experts claim that Stuxnet achieved just that, delaying the Iranian nuclear program by about two years. They add that Stuxnet is so complicated that it might have taken years to develop and required resources that are only available to governments.[xviii], [8] The significance of *Stuxnet is* that it can be regarded as *the first manifestation of Western cyber power projection capabilities*. Its main attribute is its high sophistication, compared to the relatively simple technology utilized by DDOS attacks originated from Russia and other Eastern powers.[9]

As Stuxnet shows, *purposely-designed malware multiplies the effectiveness and the reach of a cyber attack*. Thus, it is not too far-fetched to theorize that *a hypothetical armed struggle between peer great power opponents would employ both DDOS and purposefully-designed malware attacks, physical attacks on critical information infrastructure, and INFOOPS fully integrated in the operations of conventional military hardware*.

The institution that best represents the maturing Western cyber power projection capabilities is USCYBERCOM, a United States armed forces sub-unified command subordinate to the United States Strategic Command. USCYBERCOM reached full operational capability 3rd November 2010. USCYBERCOM is located in Fort Meade, Maryland under the command of General Keith B. Alexander, who also holds the title of Director, National Security Agency (NSA).[xviii] USCYBERCOM incorporates existing cyber commands of US armed forces services: Army Forces Cyber Command (ARCYBER), the 24th Air Force, Fleet Cyber Command (FLTCYBERCOM), and Marine Forces Cyber Command (MARFORCYBER). USCYBERCOM conducts both cybersecurity – in conjunction with the Department of Homeland Security (DHS)[xix] and the NSA – and INFOOPS. "*USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified Department of Defense (DoD) information networks and prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries*."[xx]

The creation of USCYBERCOM is clearly a response by the United States to hostile or unwanted activities by other nations in cyberspace. James N. Miller, Principal

[xviii] Sources: Israeli Test on Worm Called Crucial in Iran Nuclear Delay, The New York Times (January 2011).; US and Israel were behind Stuxnet claims researcher, BBC (March 2011).
[xviii] NSA is an intelligence agency of the DoD responsible for SIGINT operations. NSA is the largest SIGINT organization of the world.
[xix] DHS's National Cyber Security Division (NCSD) is the primary agency in the United States focusing on civilian cybersecurity.
[xx] Source: U.S. Cyber Command Fact Sheet, Department of Defense, 25.05.2010.

Deputy Under Secretary of Defense for Policy stated after USCYBERCOM reached initial operational capability in May 2010 that DoD had about 15 000 computer networks consisting seven million computers worldwide. According to Miller, over a hundred foreign intelligence services are attempting to conduct CNO against DoD networks, scanning them "thousands of times" an hour. He added that some countries are developing INFOOPS capabilities.[xxi] USCYBERCOM commander Gen. Alexander in 2010 said that the number of daily CNO attacks against DoD systems were 250 000 an hour, adding that between 10 terabytes and 20 terabytes of information was remotely removed. He added the China and Russia are "near peers" of the United States in CNO capabilities.[xxii]

Chinese cyber power

Chinese INFOOPS is based on what international experts widely recognize as the most powerful CNO capabilities in the world, supported by substantial SIGINT resources. The huge amount of information gathered through Computer-Network Exploitation and SIGINT is evaluated and analyzed by vastly numerous personnel facilitated by Chinese demographics. Chinese intelligence and cyber intelligence utilize the method of *mosaic intelligence*, which aims at acquiring as much information as possible for later procession. Chinese INFOOPS capabilities have a huge role in acquiring military and civilian high-technology. At the same time, INFOOPS directly helps closing the capability gap between the People's Liberation Army and advanced Western militaries. By 2030, China's overall INFOOPS capabilities may be world-leading.[10]

Chinese CNO is coordinated and directed by various government agencies, but is based on botnets operated by organized criminals and the great numbers of patriotic hackers integrated into various groups, the biggest being the Red Hacker Alliance willing to work for the government. Chinese malicious software endanger practically any computer connected to the internet, meaning that computers directly executing Chinese CNO can be physically located in any country, making it extremely difficult to trace back the origins of a Chinese cyber attack. Computers and other IT products manufactured in China are often infected with malware before leaving the factory. The main targets of Chinese CNO are foreign governments, militaries, defense and other high-tech companies.[11, 12]

[xxi] Sources: Pentagon says military response to cyber attack possible, Agence France-Presse (May 2010); Policy Official Notes Cybersecurity Challenges, Department of Defense (May 2010).
[xxii] Source: Cyber Threat to Pentagon is Global: China, Russia Near Peers of US, www.geostrategy-direct.com (October 2010).

Besides intelligence gathering, the military is utilizing CNO as part of INFOOPS as well. Chinese INFOOPS units are capable of attacking enemy information networks with malware, while protecting own forces against cyber attacks. Since 2005, the PLA has routinely built INFOOPS into its major exercises.[13] The first document emphasizing the importance of INFOOPS was the Defense White Book published in December 2004. All subsequent White Books (the last was published in March 2011) are highlighting INFOOPS and Network-Centric Warfare the Chinese collectively call these the "informationization" of the armed forces as essential in building a world-class military. In early 2010, President Hu Jintao announced that investment in INFOOPS would be a high priority during the 2011–2015 Five Year Plan.[14]

INFOOPS plays a pivotal role in the unfolding "cold war" between the United States and China for the domination of the Western Pacific. Both American and Chinese military doctrine builds heavily on INFOOPS. INFOOPS is considered a basis for the growing Chinese capabilities to execute non-nuclear first strike against American and Allied military assets in the Western Pacific theatre of operations. Air-Sea Battle, a military doctrine under elaboration by the DOD reportedly recognizes this and gives INFOOPS a vital role in Allied military operations.[15]

The PLA's INFOOPS activities had until recently been decentralized in the Third and Fourth Departments in the PLA General Staff Department (GSD)[xxiii] and specialized bureaus attached to military regions. The Third PLA GSD Department (*Technical Department*) is responsible for SIGINT operations, and also monitors internal PLA communications as well as civilian international communications to and from China. The Technical Department is the third largest SIGINT organization in the world, after those of the United States and Russia. The Fourth Department (*Electronic Countermeasures & Radar Department*) is responsible for developing equipments, doctrines, and tactics for EW and other areas of INFOOPS.[xxiv] The existence of the PLA's *Information Security Base* was reported in the Chinese media in July 2010 and is under the command of the PLA GSD. The Information Security Base is believed to be the Chinese counterpart of the USCYBERCOM, coordinating the various units already conducting INFOOPS. The Chinese cyber command is tasked with both cybersecurity and INFOOPS, with a strong focus on military cyber espionage.[16]

Although both the Third and Fourth PLA GSD Departments and the Information Security Base share the duty of cyber intelligence as part of their overall INFOOPS

[xxiii] The GSD is the most important of the PLA's general departments. It carries out staff and operational functions of the PLA and holds significant responsibility for implementing military modernization plans. Source: IHS Jane's.

[xxiv] Source: www.sinodefence.com/overview/organisation/gsd.asp, Retrieved 09.06.2011.

operations, specialized military cyber intelligence activities are conducted by the Bureau of Science and Technology or "seventh bureau" of the GSD Second Department (*Military Intelligence*). "*This is where China's vaunted "cyberintelligence" operations are designed and managed with the help of six government-linked research institutes, two computer centers and legions of patriotic citizen hackers. The bureau includes companies that produce electronic equipment – computers, satellites, listening devices and such – for espionage and technical support.*"[17]

Russian cyber power

Russia is the other non-Western nation that possesses significant cyber power. It is the only nation that has launched a cyber power attack against another country, furthermore so far only Russia has proven its ability to effectively integrate INFOOPS with conventional military operations in an actual war against a nation-state. Russia widely utilizes CNO against countries it considers to be part of its area of influence (countries that were part of the Soviet Union), complementing energy diplomacy, secret service activities, supporting unstable governments with cash and protection, stationing military forces, etc. to maintain Russian leverage in these countries. At the same time, much like China, Russian Counter-Network Exploitation capabilities are directed at Western state, military and high-tech company information systems as part of overall Russian espionage efforts.

Russian INFOOPS capabilities are based on botnets principally operated by criminal groups.[18] Complementing that, Russian "black hat" hacker groups are considered to be world leaders in computer software cracking,[xxv] and the creation and utilization of rootkits.[xxvi] These groups operate with the tacit approval of the government, and earn their income by various cybercrime activities directed at Western cyberspace. In exchange for their freedom of operations, Russian criminal gangs are obliged to direct their botnet-enabled CNO capabilities at targets deemed fit by the government. The Russian Business Network (RBN) is the best known cybercrime group, whose botnets took part in DDOS attacks against Estonia. RBN has direct personal links to the Russian government and security services.[19] At the same time, the Russian secret services are covering their INFOOPS activities by establishing fake companies and mimicking the methods and structure of the RBN.[20]

[xxv] Cracking is the process aimed at circumventing or bypassing copyright protection on software and digital media.

[xxvi] A rootkit is a collection of malicious software that enable administrator-level access to a computer or computer network, installed after first obtaining user-level access.

INFOOPS plays a key role between the struggle between Russia and NATO. Russia has so far only used offensive INFOOPS capabilities against former Soviet states along its borderland with the West and where it confronts Western interests.[xxvii] Russian INFOOPS activity had a great influence on forming the new NATO Strategic Concept and one of the most powerful Russian tool in securing the Russian sphere of influence.

The Russian agencies tasked with INFOOPS are the Federal Security Service (FSB),[xxviii] the Federal Protection Service (FSO),[xxix] the Foreign Intelligence Service (SVR),[xxx] and the Main Intelligence Directorate of the General Staff of the Armed Forces (GRU).[xxxi] Of those, the FSB, the FSO and the GRU have CNO capabilities, and the FSB is the prime agency for cyber security.[21] The civilian services are all under the direct control of the President, while GRU is, albeit enjoying a great degree of autonomy, structured under the Ministry of Defense.

The chief Russian cybersecurity agency is the Signals Intelligence Directorate of the FSB. The Directorate was formally known as the Federal Agency of Government Communications and Information (FAPSI),[xxxii] and had traditionally specialized in SIGINT and EW, coordinating and sharing assets with the GRU. After reforming Russian secret services, the FAPSI was incorporated to the FSB. FSB thus took responsibility for licensing and overseeing internet links and mobile phone communications in Russia and many other CIS countries. At the same time, FAPSI's SIGINT assets deployed against foreign states were transferred to the GRU. The Signals Intelligence Directorate is also responsible for the security of telecommunications and information systems of the federal and the regional governments.[xxxiii] FSB's Chief Directorate 'Service A' performs PSYOPS duties ('maskirovka'), disseminating false information.[21]

The Special Communication and Information Service of the FSO performs Computer-Network Exploitation tasks. The FSO also took over SIGINT assets from FAPSI, and supervises top-level communications.

[xxvii] Estonia is a NATO member, Georgia has built extensive security partnership with NATO and the United States, while the main purpose behind the 18th June 2009 cyber attack against Kyrgyzstan was the successful persuasion of the Kyrgyz government to deny access to the Manas Air Base for United States Air Force. Before that, Manas played a key role in the Afghanistan air bridge.
[xxviii] Federal'naya Sluzhba Bezopasnosti.
[xxix] Federalnaya Sluzhba Okhrana.
[xxx] Sluzhba Vneshney Razvedki.
[xxxi] Glavnoye Razvedovatel'noye Upravlenije.
[xxxii] Federal'naya Agenstvo Pravitel'stvennoy Svayazi i Informatsii.
[xxxiii] Source: IHS Jane's (June 2010).

The SVR's main focus is human political and economic intelligence and industrial espionage, but it also has foreign SIGINT capabilities. According to USCYBERCOM commander Gen. Keith Alexander, "a foreign intelligence service" believed to be Russia's SVR managed to bridge the physical separation of classified networks from non-classified networks, using a secret operative to enable cyber espionage against US military networks.[xxxiv]

The 6th Directorate of the GRU operates the Russian military's SIGINT assets. The GRU also performs CNO. GRU, along with the FSB, likely played a key role in coordinating and organizing Computer-Network Attacks against Georgia during the 2008 war.[20]

Russia's INFOOPS capabilities are likely to be further strengthened after planned joint cybersecurity capabilities of the Commonwealth of Independent States (CIS) are set up. CIS plans to reach that goal by 2015.[xxxv]

Conclusion

The struggle between great powers in cyberspace is constantly evolving, but it will likely remain an important aspect without which international relations can no longer be understood. Cyberspace truly nets all levels of decision-making and execution. This new, ever-changing space has not changed the fundamentals upon which nations build their policies towards each other; it has merely added another already indispensable "tool in the box". This tool was created by China and Russia in the process of reassertion, eager to close the gap between themselves and the West. The West has finally recognized the importance of cyber power and the threat to its overall power in case cybersecurity and INFOOPS are neglected, and has successfully played catch-up with the Chinese and Russian offensive cyber capabilities.

References

1. Daniel T. KUEHL (2009): From Cyberspace to Cyberpower: Defining the Problem. In: Franklin D. KRAMER, Stuart STARR, Larry K. WENTZ (Eds): *Cyberpower and National Security* National Defense University Press, 2009.
2. Michele FLOURNOY, Shawn BRIMLEY: The contested commons. *Proceedings Magazine,* Vol. 135/7 (2009), United States Naval Institute.

[xxxiv] Source: Cyber Threat to Pentagon is Global: China, Russia Near Peers of US, www.geostrategy-direct.com (October 2010).
[xxxv] Source: Kavkaz News (November 2010).

3. Sándor MUNK: Critical infrastructure protection against cyber attacks. (A kritikus infrastruktúrák védelme információs támadások ellen.) *Hadtudomány,* April 2008.
4. *International Strategy for Cyberspace*, issued by the President of the United States, May 2011.
5. AJP 3.10, NATO Military Information Operations.
6. László KOVÁCS, Csaba KRASZNAY: A cyber attack scenario against Hungary (Digitális Mohács? Egy kibertámadási forgatókönyv Magyarország ellen), *Nemzet és Biztonság* (February 2010).
7. *Cyber-War!* Georgian Foundation for Strategic and International Studies (November 2010).
8. James P. FARWELL, Rafal ROHOZINSKI (2011): Stuxnet and the Future of Cyber War. *Survival,* 53, Global Politics and Strategy, International Institute of Strategic Studies:23–40.
9. Alexander KLIMBURG (2011) Mobilising Cyber Power. *Survival,* 53, Global Politics and Strategy, International Institute of Strategic Studies, 53, 2011, pp. 41–60.
10. Military Power of the People's Republic of China 2009, A report to Congress pursuant to the National Defense Authorization Act, Fiscal Year 2000, Office of the Secretary of Defense, Washington DC, 2009.
11. *China: Cybersecurity and Mosaic Intelligence*, Stratfor (August 2008).
12. *China: Pushing Ahead of the Cyberwarfare Pack*, Stratfor (March 2009).
13. Zsolt HAIG, István VÁRHEGYI: Interpreting cyberspace and cyber warfare. (A cybertér és a cyberhadviselés értelmezése.) *Hadtudomány*, February 2008.
14. Jan VAN TOL (2010): AirSea Battle: A Point of Departure Operational Concept, Center for Strategic and Budgetary Assessments.
15. Ross BABBAGE (2011): *Australia's Strategic Edge in 2030*, Kokoda Foundation.
16. Russell HSIAO (2010): China's Cyber Command? *China Brief*, 10, The Jamestown Foundation.
17. *Special Report: Espionage with Chinese Characteristics*, Stratfor (March 2010).
18. Phil WILLIAMS (2002) *Organized Crime and Cyber-Crime: Implications for Business*, Carnegie Mellon University Software Engineering Institute.
19. Kara FLOOK (2009): *Russia and the Cyber Threat*, American Enterprise Institute Critical Threats.
20. *Project Grey Goose Phase II Report: The evolving state of cyber warfare*, Greylogic (March 2009).
21. Roland HEICKERÖ (2010) *Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations*, Swedish Defence Research Agency.