Cyber an operational domain of warfare, and Militaries establishing Cyber commands and planning Offensive cyber operations

The incidents of cyberwarfare are ever increasing, targeting more and more countries and becoming legitimate. Part of the Ukrainian power grid was attacked by hackers, causing blackouts; US accused Iranians of attempting to hack into the control-system of a dam. President Barack Obama strongly suggested that Russian President Vladimir Putin personally authorized the computer hacks of Democratic Party emails that American intelligence officials say were aimed at helping Republican Donald Trump win the Nov. 8 election. Russia was also suspected for cyber-attack on Turkey following the downing of a Russian fighter jet late last year. The US Government itself has announced to have launched a series of cyber-attacks against the Islamic State coordinated by the Cyber Command. “Our cyberoperations are disrupting their command-and-control and communications,” Mr. Obama saidat the C.I.A. headquarters in Langley, Va., on countering the Islamic State.

“At its heart, cyberwarfare involves digital attacks on the networks, systems and data of another state, with the aim of creating significant disruption or destruction. That might involve destroying, altering or stealing data, or making it impossible to access online services, whether they are used by the military and broader society. These digital attacks may also be designed to cause physical damage in the real world –

such as hacking into a dam's control systems to opening its floodgates," says Techrepublic. A wider definition of cyberwarfare could also include some elements of what is also known as information warfare – including online propaganda and disinformation, such as the use of 'troll armies' to promote a certain view of the world across social media.

"Cyber warfare is a great alternative to conventional weapons," says Amy Chang, a research associate in the technology and national security program at the Center for a New American Security. "It is cheaper for and far more accessible to these small nation-states. It allows these countries to pull off attacks without as much risk of getting caught and without the repercussions when they are [caught]."

NATO ministers have designated cyber as an official operational domain of warfare, along with air, sea, and land. Cyber warfare has developed into a more sophisticated type of combat between countries, where you can destroy communications infrastructure, said Marc Rogers, Head of Security for DefCon, adding that ordinary people become pawns in these games. Many governments are building a cyberwarfare capability: among the most advanced countries are the US, Russia, China, Iran and South Korea. US and other coutries including U.K., China, Russia, Israel and others are setting up Unified cyber commands for more effective and coordinated efforts for conducting cyberspace operations, both offensive and defensive. The offensive operations are seen as deterrent to adversaries.

Sergei Shoigu Russia's defense minister in Feb 2017 made first official acknowledgement of the existence of Russian cyber army when he said that his nation also has built up its

muscle by forming a new branch of the military – information warfare troops. Retired Gen. Vladimir Shamanov, the head of defense affairs committee in the lower house of parliament, said that information warfare troops' task is to "protect the national defense interests and engage in information warfare," according to the Interfax news agency. He added that part of their mission is to fend off enemy cyberattacks. Viktor Ozerov, the head of the upper house's defense and security committee, also told Interfax that the information troops will protect Russia's data systems from enemy attacks, not wage any hacking attacks abroad.

The US Unified Cyber command, USCYBERCOM

"The breadth of cyber threats posed to U.S. national and economic security has become increasingly diverse, sophisticated, and impactful," Director of National Intelligence James Clapper said. "Although we must be prepared for a large, armageddon-scale [attack] that would debilitate U.S. infrastructure, that is not the most likely scenario," Clapper told the committee. "We foresee an ongoing series of low-to-moderate level cyberattacks from a variety of sources over time, which impose cumulative costs on U.S. economic competitiveness and national security."

"The first shots of the next actual war will likely be fired in cyberspace and likely with devastating effect," Chief of Staff Gen. Milley said at the event. "Many analysts and senior government officials have said their greatest fear is a cyber Pearl Harbor. Paul Nakasone's father was at Pearl Harbor as a 14-year-old young man. We never want to see that day happen again.""Army Cyber is racing the clock literally every day to stay ahead of adversaries in cyberspace," said the Army's top officer, Gen. Mark Milley.

Chairman Sen. John McCain, R-Ariz., attributed America's diminished cyber defenses to the lack of a policy on deterrence. "Our adversaries view our response … as timid and ineffectual. Put simply, the problem is a lack of deterrence. The administration has not demonstrated to our adversaries that the consequence of continued cyberattacks against us outweigh the benefit."

On March 17 2016, Secretary of Defense Ash Carter testified before Congress that the Pentagon is actively ramping up its cyber and electronic warfare divisions, including $34 billion appropriated exclusively for the new cyber and electronic divisions. On June 23, 2009, the Secretary of Defense directed the Commander of US Strategic Command (USSTRATCOM) to establish a sub-unified command, USCYBERCOM. The increase in the number and sophistication of attacks on the US' cyber networks is necessitating more effective and coordinated efforts for conducting cyberspace operations, according to US Army officials. US Defense Secretary Ash Carter's new cyber-strategy acknowledges that the Pentagon may wage offensive cyber-warfare.

U.S. Cyber Command is split off from the intelligence-focused National Security Agency. The goal, they said, is to give U.S. Cyber Command more autonomy, freeing it from any constraints that stem from working alongside the NSA. Making cyber an independent military command will put the fight in digital space on the same footing as more traditional realms of battle on land, in the air, at sea and in space. The move reflects the escalating threat of cyberattacks and intrusions from other nation states, terrorist groups and hackers, and comes as the U.S. faces fears about Russian hacking.

U.S. Cyber Command is composed of several service components, units from military services who will provide Joint services to Cyber Command. In March the Cyber Mission Force was said to be at about half of its target of 6,187 personnel in 133 teams, to be divided among the nation mission force, the combat mission teams and cyber-protection teams. Each service has a two- or three-star headquarters whose commander provides forces both to their service and Cyber Command when they are supporting other joint forces headquarters.

The USCYBERCOM conducts and synchronizes activities to: secure, operate, and defend the DODIN; attain freedom of action in cyberspace while denying same to adversaries; and, when directed, conduct full spectrum cyberspace operations in order to deter or defeat strategic threats to U.S. interests and infrastructure, ensure DoD mission assurance, and achieve Joint Force Commander objectives.

US's CYBERCOM, which has overall authority over the 133 teams the military services are building certified that the Army's 41 teams of active-duty soldiers and civilians had reached full operational capability (FOC) on Sept. 28 2017. A similar validation for the Navy's 40 teams followed on Oct. 6, officials said. Each of the services is expected to have its teams achieve the FOC stage by Sept. 30, 2018, and each declared initial operating capability (IOC) in October of last year.

"Reaching FOC at this point in the development of the Navy's CMF teams is a testament to the extraordinary hard work invested in manning our teams and training our personnel,"

Vice Adm. Michael Gilday, the commander of the Navy's 10th Fleet/Fleet Cyber Command, said in a statement. But he cautioned that the FOC declaration – coming after 1,800 personnel had completed some 18,000 courses – does not mean the Navy has come close to meeting all of its objectives when it comes to equipping and training its cyber workforce, and is not a measure of overall "combat readiness."

The US Army will soon send teams of cyber warriors to the battlefield as the military increasingly looks to take the offensive against enemy computer networks. While the Army's mission is generally to 'attack and destroy,' the cyber troops have a slightly different goal, said Colonel Robert Ryan, who commands a Hawaii-based combat team. 'Not everything is destroy. How can I influence by non-kinetic means? How can I reach up and create confusion and gain control?' he told reporters. The cyber soldiers have been integrated for six months in infantry units, and will tailor operations according to commanders' needs, said Colonel William Hartman of the Army's Cyber Command.

Pentagon has already finalized "Rules of Engagement" for Cyber Warfare which will allow military commanders to determine when the cyber-attack constitutes a "Act of War". It will also provide a framework so that the military can take appropriate actions

The US Army Network Enterprise Technology Command has activated the Cyber Protection Brigade expected to provide a more agile and responsive cyberspace force. The brigade would include platoon-sized cyber protection teams comprising soldiers, non-commissioned officers, officers, warrant officers, as well as the Army civilian employees. It would

comprise of multiple teams, overall 41 teams, focusing on defending DoD's own networks, defending civilian critical infrastructure and offensive operations.

US Navy's ninth type command (TYCOM), Information Dominance Forces Command, supports integration of Information Dominance ID capabilities throughout the Navy. The navy's plan is even more comprehensive than Army's as they say they plan to integrate the space cadre and oceanographers, in addition to Intelligence specialists, information warfare officers and information professionals.

The creation of U.S. Cyber Command appears to have motivated other countries in this arena.

UK establishes British Cyber Command to Attack ISIL

Britain spies will be able to launch "offensive" cyber-attacks on individual hackers, criminal gangs and rogue states as well as jihadists for the first time under new techniques being developed by the intelligence agencies, George Osborne has revealed.

"Strong defences are necessary for our long-term security. But the capacity to attack is also a form of defence. "We need not just to defend ourselves against attacks, but rather to dissuade people and states from targetting us in the first place. "Part of establishing deterrence will be making

ourselves a difficult target, so that doing us damage in cyberspace is neither cheap nor easy. “And part of establishing deterrence will be making sure that whoever attacks us knows we are able to hit back. “We are building our own offensive cyber capability – a dedicated ability to counter-attack in cyberspace.”

According to The Guardian, the 77th brigade formally came into being in April 2015. It was established as a special unit within its military structure – the British Cyber Command, by transferring up to 1500 officers under its command. The brigade will be carrying out covert operations on social networks exclusively, in an effort to spread disinformation and manipulate the population of certain countries, which should create “favorable conditions” for applying political pressure or the executing of regime change in strategically important regions of the world.

China unifying cyber warfare capabilities under a centralized command “Strategic Support Force (SSF)”

China’s rival to U.S. Cyber Command, the ambiguously named Strategic Support Force (SSF) was founded in 2015, and today responsible for conducting many of Beijing’s most sensitive cyber-espionage and propaganda missions. A recently released unclassified report by the Defense Department concerning the state of the PLA highlights the importance of the SSF in the scope of Beijing’s quest to challenge the U.S. in cyber and space weapons development.

“Chinese leadership has described the SSF as a ‘new-type’ force and force for innovation, incubating some of the [People

Liberation Army]’s most advanced capabilities, meaning it will be earmarked significant resources,” said John Costello, a senior analyst with U.S. dark web intelligence firm Flashpoint. “The SSF reflects a broader conception of cyber operations than that assumed by U.S. armed forces,” said Segal, specifically by Cyber Command. For example, information operations, also known as psychological warfare, is aligned with China’s offensive cyber mission because of the way Chinese military officials generally understand cybersecurity.

China established “information warfare units in the People’s Liberation Army (PLA) in 2003 and in the 2004 it prioritized of using information to fight and win wars. In 2010, China introduced its first department dedicated to defensive cyber war and information security, in response to the creation of USCYBERCOM. The PLA’s first specialized information unit was set up in July 2010, not long after the U.S. Cyber Command went operational.

Segments of the country’s 3PLA, China’s version of the NSA, and 4PLA, a clandestine unit responsible for electronic warfare and information operations, were consolidated into the SSF two years ago. China’s military chiefs unified the country’s cyber warfare capabilities under a centralized command reporting to the Central Military Commission. This would better organize China’s cyber warfare capabilities and enhance the role of cyber within the PLA. A unified command would be “a pretty big deal” in organizing domestic cyber forces to “win informationized local wars,” according to Council on Foreign Relations cyberspace program director Adam Segal.

“It would be an official sign that cyber-attacks would be used

in a military conflict," he said. "Theoretically, it would allow them to concentrate resources in one place and create specialized forces, and might make it easier to plan joint operations." Rep. Mike Pompeo (R-Kan.) said that China, through the PLA, has developed one of the most sophisticated cyber capabilities in the world.

China's government is sharply increasing its investment in cyber warfare programs in what U.S. intelligence officials say is a major attempt to compete with superior U.S. military cyber capabilities. The boost in Chinese cyber warfare programs followed a meeting in September of the ruling Communist Party Politburo when General Secretary and President Xi Jinping called for adopting a new information warfare strategy.

State-run Chinese television reported Sept. 2 that President Xi Jinping called for "more military innovation in China and a new strategy for information warfare amid a global military revolution." The directive was made during an Aug. 29 meeting of the Communist Party Politburo.

North and South Korea

The South Korean government has admitted that its cyber military command was hacked in Sep 2016 by injecting malicious codes into one of its main routing servers. South Korea's military cyber command, set up to guard against hacking, has said. "It seems the intranet server of the cyber command has been contaminated with malware. We found that some military documents, including confidential information, have been hacked," a military spokesman told South Korea's Yonhap news agency.

North Korea is believed to have thousands of personnel involved in cyberwarfare. Since 2010 they have been focusing on application programming interfaces (APIs), which can be designed to attack national infrastructures, North Korean defector and computer science professor Kim Heung-Kwang told the BBC.

A formal investigation has begun into the hack and its origin. Among those suspected, the first finger is being pointed at the North. “North Korea began to train its cyber warriors while developing nuclear arms in the early 1990’s and now commands 1,700 highly skilled and specialised hackers,” Cho Hyun Chun, chief of South Korea’s Defence Security Command had said earlier.

In mid-June, South Korean police reported that more than 140,000 computers at 160 South Korean firms (mostly defense contractors) were hacked by North Korean hackers. During those attacks, more than 40,000 defense-related documents were stolen.

In December 2009, South Korea announced the creation of a cyber warfare command. Reportedly this is in response to North Korea’s creation of a cyber warfare unit. Little is known about the structure of North Korea’s cyber warfare operations, and the regime has said previously it’d retaliate against any U.S. provocations with conventional, nuclear and cyber-attacks.

Taiwan’s “Cyber Army” Plan

Taiwan’s new Minister of National Defense Feng Shih-kuan (□□□) recently confirmed the intention of the new government to create a “Cyber Army” (□□) as the fourth branch of Taiwan’s armed forces. The announcement followed the plan outlined in the Defense Policy Blue Papers published earlier by the Democratic Progressive Party (DPP), which specifically called for the “[Integration of] existing military units and capacities of IT, communications, and electronics to establish an independent fourth service branch alongside the current Armed Forces consisting of the Army, Navy, and Air Force.” Taiwan’s plan for a Cyber Army however, will make it the first country to assign equal importance to cybersecurity as to the other branches of the armed forces.

Taiwan has been target of cyber-attacks from china since many years, and has been a “testing ground” for China’s cyber army and state-sponsored hackers according to Taiwanese officials.

Germany prepares for cyberwarfare offensive

Germany’s military, the Bundeswehr, is a high-value target for hackers and foreign spy agencies – not only because of its military secrets, but also due to its IT-supported weapons systems. If hackers were ever to gain control of them, the results could be devastating.

Future cyber attacks are to be fended off by the new “Cyber and Information Space Command” (CIR), which will become operational on April 1. The command will have its own independent organizational structure, thus becoming the sixth branch of the German military – on a par with the army, navy,

air force, joint medical service and joint support service. Eventually, 13,500 German soldiers and civilian contractors currently dealing with cyber defense from a number of different locations will be brought together under the CIR’s roof.

The Bundeswehr is facing a major change of its strategy in cyber warfare. In addition to defense against cyberattacks, the German army is due to perform attacks on foreign states, DWN wrote, referring to a strategy paper of the German Ministry of Defense. The Bundeswehr will be responsible for responding to cyberattacks – while also resorting to military means in case of attack on its critical infrastructure such as communication and transport networks. The guidelines include not only defensive measures but also offensive ones. The Bundeswehr will be ready to carry out offensive cyber operations in Germany as well as abroad.

Establishing an IDF Cyber Command

IDF Chief of Staff Gadi Eisenkot said that, in light of the challenges the IDF faces in the cyber sphere, a cyber command should be established in order for it to oversee all operational activity in the cyber dimension. According to the IDF Spokesperson’s Unit, the new command will be established over a time period of two years.

The announcement of the new cyber command came a day after Israeli cybersecurity company ClearSky said it had uncovered a massive Iranian cyber-attack against Israel. Attacks were launched against 40 Israeli targets and 500 other targets worldwide, including against reserve generals in the IDF, a security consulting company, and researchers, the firm told

Army Radio.

IDF cyber command will be directly subordinate to the Chief of Staff; the fifth such branch after, the air force, navy, and intelligence, charged with both the buildup and the operational missions of the force. The major imperative in coherently implementing the decision to set up a cyber command within the IDF will be the attainment of maximal operational cooperation between the new command and other IDF forces and units.

Meir Elran and Gabi Sibonisay in INSS note: “This will not be an easy undertaking. A particularly important challenge will be the attainment of both long range planning and precise execution capabilities on the different levels, together with an optimal degree of operational flexibility in the defensive and offensive theater. An improved, innovative cyber system will serve to expand Israel’s spectrum of security capabilities, as long as it is integrated with an updated general security doctrine that is responsive to Israel’s rapidly changing needs.”

Iran scaling up their cyber capabilites

Hackers probably linked to Iran’s government have hit Saudi and Western aerospace and petrochemical firms, marking a rise in Iranian cyber-spying prowess, security firm FireEye (FEYE.O) said on Wednesday, an assessment shared by other U.S. experts.

Iran has been scaling up its cyber capacities since the United States and Israel carried out a cyber assault on Iran in 2010, now known as the “Stuxnet” worm, aimed at disabling

centrifuges in its nuclear programme, he said.

Speaking to reporters in Singapore, FireEye Chief Executive Kevin Mandia said Iranian cyber espionage had grown in sophistication since he first spotted Iranians conducting rudimentary attacks on the U.S. State Department in 2008. “They’re good. (They‘ve) got a real capability there,” Mandia said of Iran. In the investigations of attacks on Western companies and governments that FireEye is hired to do, Iran now ranks with China and Russia in terms of frequency, he said.

“In recent years, Iran has invested heavily in building out their computer network attack and exploit capabilities,” said Frank Cilluffo, director of George Washington University’s Center for Cyber and Homeland Security. Cilluffo, a former homeland security advisor to President George W. Bush, estimated last year in testimony before the U.S. Congress that Iran’s cyber budget had jumped twelve-fold under President Rouhani, making it a “top five world cyber-power”.

“They are also integrating cyber operations into their military strategy and doctrine,” he told Reuters on Wednesday.

References and Resources also include:

- http://www.marketwatch.com/story/this-is-south-koreas-elite-cyber-army-that-fights-north-korea-2016-06-30
- http://blog.project2049.net/?utm_source=AsiaEye+Blog+-+Taiwan%27s+%22Cyber+Army%22+Plan&u
- http://www.israelnationalnews.com/News/News.aspx/208126
- http://www.zdnet.com/article/cyberwarfare-comes-of-age-the-internet-is-now-officially-a-battlefield/
- http://www.techrepublic.com/article/cyberwar-the-smart-persons-guide/

- http://securityaffairs.co/wordpress/46656/terrorism/cyber-attacks-against-islamic-state.html
- https://www.armytimes.com/articles/new-commander-at-army-cyber-command
- http://www.ibtimes.co.uk/south-korean-military-cyber-command-hacked-by-injecting-malicious-codes-into-routing-server-1584471
- http://abcnews.go.com/International/wireStory/russian-military-continues-massive-upgrade-45652381
- http://www.thehindu.com/news/international/us-cyber-command-to-be-revamped/article19286099.ece
- http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517
- https://www.cyberscoop.com/china-ssf-cyber-command-strategic-support-force-pla-nsa-dod/
- https://www.reuters.com/article/us-iran-cyber/once-kittens-in-cyber-spy-world-iran-gains-prowess-security-experts-idUSKCN1BV1VA