US, China and Russia developing new cyber capabilities and technologies like Secure Internets to protect against Cyber Warfare

Cyber warfare has developed into a more sophisticated type of combat between countries, where you can destroy critical infrastructure such as power, telecommunications or banking by damaging the computer systems that control those infrastructures. It's widely acknowledged that offensive cyberattacks will be a necessary component of any future military campaign, and the extreme cyberweapons are being developed now. The United States has been accusing Chinese government and military of cyber attacks against U.S. government computer systems. Beijing denies those claims and also says it is a victim of hacking.

Many countries starting with US and which now includes 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. US, Russia and China are also implementing various defence measures to protect their Classified networks from Cyber Warfare.

The PLA Daily has made it clear that China's "cyber territory" must be defended as vigorously as physical territory. "If China doesn't occupy and defend its "cyber territory," then

nameless “hostile forces” will use it as a “bridgehead” to attack China. “ The control of cyberspace means for the 21st century what control of the maritime domain meant for the 19th and air and space superiority meant for the 20th century.”

China has built its own internet, the “Great Firewall” that blocks many social media services, such as Twitter, Facebook, YouTube, Instagram, Snapchat and Google, along with many rights groups sites and some foreign media agencies.

US has developed SIPRNet, or Secret Internet Protocol Router Network, global military Internet system used for transmitting classified information, intelligence, targets, and messages at the secret level. In other words, SIPRNet is completely parallel Internet, uses the same communications procedures and has been kept separate from the ordinary civilian Internet.

Russia is another among of only a handful of countries to have developed its own internet, including its own search engines, e-mail systems, and social networks. Russian military forces have completed the creation of own electronic communication system that is completely independent from the internet and protected from unlicensed connections, allowing for fast and safe transfer of classified information.

Russian presidential adviser for internet issues, German Klimenko, said in comments that he considered it correct that the Closed Data Transfer Segment has absolutely no connection to the internet. “Anything that is connected can be broken

into and therefore is not safe," he said.

"Americans have had quite a lot of holes in their network. They were changing network protocols on-the-go and besides, they had a lot of separate networks for every branch of forces and lastly – their system has too many connection points with the internet, which raises the danger of unsecure access," he said.

"As far as I understand, Edward Snowden has been working for one of the NSA's subcontractors and had access to this network which allowed him to gain access to the data that he made public. I hope our people have not made similar mistakes when they planned the network and that they have taken additional security measures."

China's Internet Security Measures

China recently said that it will create a national data repository for information on cyber attacks and require telecom firms, internet companies and domain name providers to report threats to it. The Ministry of Industry and Information Technology (MIIT) said companies and telcos as well as government bodies must share information on incidents including Trojan malware, hardware vulnerabilities, and content linked to "malicious" IP addresses to the new platform.

An MIIT policy note also said that the ministry, which is creating the platform, will be liable for disposing of threats under the new rules, which will take effect on Jan. 1. Companies and network providers that fail to follow the rules will be subject to "warnings, fines and other administrative penalties", it said, without giving any

details.

“The building of national defense cyberspace capabilities is an important part of China’s military modernization,” the Foreign Ministry and the Cyberspace Administration of China, the country’s internet regulator, said in a strategy for global online cooperation on the ministry’s website. China will help in the military’s important role in “safeguarding national cyberspace sovereignty, security and development interests” and “hasten the building of cyberspace capabilities”, the strategy said, but also called on countries to “guard against cyberspace becoming a new battlefield.”

China has built Great Firewall to keep unwanted foreign influences out of China. The result is a balkanized Internet within China, known as the Chinternet or Great Chinese LAN. The OpenNet Initiative performed an empricial study that concluded that China has “the most sophisticated content-filtering Internet regime in the world”. Some technical methods used are IP blocking, which denies the IP addresses of specific domains, packet filtering, which scans packets of data for controversial keywords, credit records, and speech and facial recognition.

China has installed a secure operating system known as “Kylin” on government and military computers designed to be impenetrable to US military and intelligence agencies. Kevin Coleman, a private security specialist said its deployment is significant because it has “hardened” key Chinese servers. “This action also made our offensive cyber capabilities ineffective against them, given the cyber weapons were designed to be used against Linux, UNIX and Windows,” he said, citing three popular computer operating systems.

At the beginning of 2014, an alliance of fifteen private Chinese IT manufacturers was founded in the Beijing district of Zhongguancun (□ □ □), the Chinese equivalent of Silicon Valley. They stepped up endeavours to develop a Chinese operating system based on Linux that would run on government computers and the computers of security relevant businesses such as banks. By taking this step, Beijing hopes to gain protection from espionage from the USA and demonstrate the innovative power of the Chinese IT economy.

The Chinese have also developed a secure microprocessor that, unlike US-made chips, is known to be hardened against external access by a hacker or automated malicious software, Coleman said. “If you add a hardened microchip and a hardened operating system, that makes a really good solid platform for defending infrastructure,” he said.

An important characteristic of the Chinese internet is that online access routes are owned by the PRC government, and private enterprises and individuals can only rent bandwidth from the state. The first four major national networks, namely CSTNET, ChinaNet, CERNET and CHINAGBN, are the “backbone” of the mainland Chinese Internet. Later dominant telecom providers also started to provide Internet services. In 2015 January, China added seven new access points to the world’s Internet backbone, adding to the three points that connect through Beijing, Shanghai, and Guangzhou.

According to Xinhua, the state news agency, ninety per cent of its microchips and sixtyfive per cent of its firewall products originated in other countries in 2012, primarily the US. The

government views foreign technology as a potential threat to national security. Covertly installed back doors enable surveillance of computers and networks, for example. Therefore, stringent constraints on the use of foreign IT products are already in place in areas critical to security.

Russian military build impenetrable CLOSED internet for Military

The official name of the network is the ‘Closed Data Transfer Segment’ and Representative of the Russian Defence Ministry explained that infrastructure of the military internet has been set on the bases of the Rostelekom infrastructure they rent, as well as on their own which is not connected to the internet.

The structure of the Russian ‘military internet’ is similar to the one of the conventional World Wide Web, but it is accessible only on computers that use the dedicated operating system developed by the Russian Military Forces. The hardware also has to be certified by the General Staff’s directorate for protection of state secrets to ensure that it is impossible to even plug in an uncertified device, including printers, scanners and flash drives.

Every military unit has servers which encrypt information, divide it into several packages and forward it. Access to these buildings is strictly limited. The main resource of the network, as well as various third-level domains can be visited through computers which operate on the Armed Forces Mobile System, and are certified by the security service of the state secret, also known as the Eighth Agency of the General Staff. The military internet also has its own mail service

that allows for strictly internal exchange of messages

The source also said that the Closed Data Transfer Segment was completed already in late summer and is now in fully functioning state, but works are under way to expand it with additional terminals in every military unit.

US Secret Internet Protocol Router Network (SIPRNet)

The Secret Internet Protocol Router Network (SIPRNet) is “a system of interconnected computer networks used by the U.S. Department of Defense and the U.S. Department of State to transmit classified information (up to and including information classified SECRET) by packet switching over the TCP/IP protocols in a “completely secure” environment.

It also provides services such as hypertext document access and electronic mail. As such, SIPRNet is the DoD’s classified version of the civilian Internet. SIPRNet is the SECRET component of the Defense Information Systems Network. Other components handle communications with other security needs, such as NIPRNet which is used for nonsecure communications, and JWICS which is used for Top Secret communications.

Among its many features, computers cleared for SIPRNet access connect to the network via secure dial-up or LAN connections, access web pages written in standard HTML using a standard web browser, can upload and download files via FTP connections,

and can send or receive email messages through SMTP services using email programs such as Microsoft Outlook. All data transmitted on SIPRNet between secure facilities must be encrypted by approved NSA encryption systems. While the public Internet can be used to transmit encrypted SIPRNet packets ("SIPR over NIPR"), no access is permitted between the two networks.

Approximately 3 Million people with secret clearances have access to SIPRNet, which includes Pentagon and military officials, Intelligence agencies, FBI, as well as diplomats in US embassies all around the World

Users are issued a username and a "strong" password (of 10 characters or more, at least two capitals, two numbers and two special symbols), which must be changed at least every 150 days. In theory at least, the user has to stay at the computer at all times while logged on, logging off even to go to the toilet or get a cup of coffee.

Again in theory, any memory stick or CD connected to a computer with Siprnet access must automatically be labelled secret and stored securely. If a personal device such as an iPod is connected it can be confiscated. In practice these multiple layers of security were relaxed to make the system as easy to use as possible.

These classified networks are definitely not connected to the Internet, but this does not mean that malware or well-resourced hackers can never found their ways into these critical networks. The network at Creech Air Force Base was

crashed in early September that impacted “critical services,” and has not been completely rebuilt, according to US government contracting records.The officials would not say whether the failure was due to internal technical faults, a cyber attack, or a state-sponsored hacker.

In the year 2008, The Pentagon acknowledged a significant cyber attack, Operation Buckshot Yankee, where a foreign intelligence agent used a USB drive to infect military computers used by the Central Command in overseeing combat zones in Iraq and Afghanistan with a specially crafted malware.

References and Resources also include:

https://www.rt.com/politics/363270-russian-military-launch-own-closed/

http://www.pravdareport.com/video/19-10-2016/135932-net-0/

http://www.merics.org/fileadmin/templates/download/china-monitor/150407_MERICS_China_Monitor_22_en.pdf

http://thediplomat.com/2015/05/chinese-military-declares-the-internet-an-ideological-battleground/

http://phys.org/news/2009-05-china-deploys.html

https://www.theguardian.com/world/2010/nov/28/siprnet-america-stores-secret-cables

http://thehackernews.com/2016/10/drone-siprnet-defence-network.html

http://www.voanews.com/a/china-warns-agains-cyber-battlefield-

in-internet-strategy/3745447.html

https://www.reuters.com/article/us-china-cyber/china-beefs-up-cyber-defenses-with-centralized-threat-database-idUSKCN1BO12K