CYBER WARFARE

WHAT'S REALLY HAPPENING?
SECTION I INTRODUCTION
CYBER SPACE, WHAT IS IT?

It is all of the computer networks in the world and every thing that they connect too and/or control such as: the world wide web, the dark web and the internet of things (IOT), plus any device that can be accessed by them (i.e. phones, cars, machinery, medical devices, utilities, electric grid water and sewage networks.
CYBER WARFARE IS ACTIONS BY A NATION AGAINST ANOTHER NATION TO PENETRATE THEIR NETWORKS AND COMPUTERS FOR THE PURPOSE OF CAUSING DISRUPTION AND/OR DAMAGE (I.E. DISABLING THE MILITARY OR CIVILIAN FACILITIES TO STALL DEFENSIVE OR OFFENSIVE ACTION)

DOMAINS OF WAR

1. Land
2. Sea
3. Air
4. Space
5. Cyberspace

ADVANTAGES OF CYBER WARFARE

- It
  - Is Low cost to implement & Anomalous
  - Is difficult to identify who attackers are foreign or domestic while occurring
  - Provides non-kinetic less violent alternatives such as messing with communications, forcing high maintenance, erasing data, and identity theft
WAR IS CONSTANTLY CHANGING!

IT JUST ADDING NEW WEAPONS

WHILE CLAIMING NOTHING IS OCCURRING.
WHAT DOES CYBER WARFARE EFFECT?

• Previous Warfare attacked
  • 1. The military, its facilities and people
  • 2. The countries infrastructure and commercial facilities harbors, airports, trains and roads

• Cyber Warfare attacks “everything”:
  • 1. The military, its facilities and people
  • 2. The countries infrastructure & Commercial facilities harbors, airports, trains and roads
  • 3. The economy, the corporations, The factories as well as the banks as well as The currencies.
  • 4. The political parties, governmental institutions
  • 5. The Society, its culture, The peoples relationships and trust
The cost of conducting a traditional kinetic attack is too high for adversaries to sustain. Traditional kinetic attacks are limited in scope and only affect the military, physical, and economic planes of a nation. In order to achieve their objectives, adversaries must turn to non-kinetic attacks, as expressed in cyber warfare. It offers adversaries greater opportunities to directly impact a nation on the political and social as well as the military, physical and economic planes of the society.
THE NEW TARGETS
<table>
<thead>
<tr>
<th>number</th>
<th>year occurred</th>
<th>country involved</th>
<th>aggressor</th>
<th>winner</th>
<th>target</th>
<th>result</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2003</td>
<td>United States</td>
<td>China</td>
<td>Cuba</td>
<td>stole data from unclassified pentagon network</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2007</td>
<td>Estonia</td>
<td>Russia</td>
<td></td>
<td>stole data from world bank</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2008</td>
<td>Georgia</td>
<td>Russia</td>
<td></td>
<td>stole data from Lockheed Martin</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2009</td>
<td>Israel</td>
<td>Palestine</td>
<td></td>
<td>shutdown financial system</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2010</td>
<td>Chinese</td>
<td>Iran</td>
<td></td>
<td>shutdown internet flooded routers</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2010</td>
<td>Iran</td>
<td>United States</td>
<td>Israel</td>
<td>Operation Olympic Games shutdown uranium concentration production</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>2012</td>
<td>eastern Europe</td>
<td>Russia</td>
<td></td>
<td>Operation Olympic Games shutdown uranium concentration production</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2013</td>
<td>South Korea</td>
<td>North Korea</td>
<td></td>
<td>Operation Olympic Games shutdown uranium concentration production</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>2017</td>
<td>world networks</td>
<td>shadow breaker</td>
<td></td>
<td>Operation Olympic Games shutdown uranium concentration production</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>2017</td>
<td>Pakistan</td>
<td>India</td>
<td></td>
<td>Operation Olympic Games shutdown uranium concentration production</td>
<td></td>
</tr>
</tbody>
</table>
SECTION II CYBER ATTACKS OR EXPLOITS
CYBER TERRORISM

Is usually done by a group of hackers to inflict fear upon the victim such as stealing their identities or their credit card information to attack other banks or stores
WHO ARE THE HACKERS?

1. Unsophisticated attackers = Script kiddies/ most numerous in local attacks (usually local police investigate)
2. Sophisticated attackers = hackers, spammers (mass e-mailers) and criminals (Usually government agencies investigate)
3. Corporate Espionage = Black hatters paid by corporations identified groups Chinese, Japanese and Europeans
4. State sponsored military and civilian agencies who perform persistent attacks (API) US, Russia, China NATO/Estonia, Israel, Korea and India
WHITE HAT COMPUTING INFORMAL
A PERSON WHO HACKS INTO A COMPUTER NETWORK IN ORDER TO TEST OR EVALUATE ITS SECURITY SYSTEMS.
"WHILE SECURITY DUDES TEND TO SPEAK IN TERMS OF BLACK OR WHITE HATS, IT SEEMS TO ME THAT NEARLY ALL HATS ARE IN VARYING SHADES OF GREY"

THE TERM "GREY HAT", ALTERNATIVELY SPelled AS "GREYHEN" OR "GRAY HAT", REFERS TO A COMPUTER HACKER OR COMPUTER SECURITY EXPERT WHO MAY SOMETIMES VIOLATE LAWS OR TYPICAL ETHICAL STANDARDS, BUT DOES NOT HAVE THE MALICIOUS INTENT TYPICAL OF A BLACK HAT HACKER. USUALLY VULNERABILITY OR INTRUSION DETECTING TESTING STAFFS

A black hat hacker (or black-hat hacker) is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain".

Black hat hackers are the stereotypically illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal". Black hat hackers break into secure networks to destroy, modify, or steal data, or to make the networks unusable for authorized network users.
TERRORIST STRIKE:

TO CREATE FEAR IN INDIVIDUALS OR SOCIETIES

To show that the organization is vulnerable usually they deface the web sites with graffiti.

---

PATTERNS OF CYBER ATTACK OR CYBER TERRORISM:

- 1\textsuperscript{st} phase of attack is reconnaissance of the intended victim. By observing the normal operations of a target, useful information can be asserted and accumulated such as hardware and software used, regular and periodic communications.

- 2\textsuperscript{nd} phase of attack is penetration. Until the attacker is inside the system, there is little that can be done to the target except to disrupt the availability or access to a given service provided by the target.

- 3\textsuperscript{rd} phase is identifying and expanding the internal capabilities by viewing resources and increasing access rights to more restricted higher value areas of a given system.

- 4\textsuperscript{th} stage is where the intruder does the damage to a system or confiscates selected data or information.

- 5\textsuperscript{th} phase is the removal of any evidence of a penetration, theft, and so forth by covering the intruder’s electronic trail by editing or deleting log files.
TRADITIONAL ESPIONAGE AND PROPAGANDA ARE NOT ACTS OF WAR. THEY ARE ASSUMED TO BE INCIDENTS

**CYBER ESPIONAGE**

- The US CIA and NSA are charged with performing and defending against espionage. They have a black budget which is not reported.

**CYBER PROPAGANDA**

- Cyber propaganda is an effort to control information in whatever form it takes, and influence public opinion. It is a form of psychological warfare, except it uses social media, fake news websites and other digital means. In 2018, Sir Nicholas Carter, Chief of the General Staff of the British Army stated that this kind of attack from actors such as Russia "is a form of system warfare that seeks to de-legitimize the political and social system on which our military strength is based".
"ECHELON" IS A SURVEILLANCE PROGRAM

- **ECHELON**, originally a secret government code name, is a surveillance program (signals intelligence/SIGINT collection and analysis network) operated by the US with the aid of four other signatory nations to the UKUSA Security Agreement—Australia, Canada, New Zealand, the United Kingdom and the United States, also known as the Five Eyes.

- The ECHELON program was created in the late 1960s to monitor the military and diplomatic communications of the Soviet Union and its Eastern Bloc allies during the Cold War, and was formally established in 1971.

- By the end of the 20th century, the system referred to as "ECHELON" had allegedly evolved beyond its military and diplomatic origins, to also become "...a global system for the interception of private and commercial communications" (mass surveillance and industrial espionage).
SECTION III THE NATIONAL PLAYERS
THE MOST POWERFUL PLAYERS IN CYBER WARFARE ARE:
UNITED STATES APPROACH TO CYBER WARFARE

• **The US Presidential Policy Directive 28 on signal intelligence activities 2014** established the overall US strategic approach to cyber warfare Missions among civilian and DOD agencies. It assigned different missions to both the existing and future agencies. The mission assignments were as follows:

  • **Defense:** The Department of defense (DOD) must be prepared to defend its own networks, systems and installations from cyber-attacks.
    - DOD must build and maintain ready forces and capabilities to conduct cyber operations, merge the 133 cyber protection teams into operational units and create specific cyber offense mission teams.
    - DOD must provide integrated cyber capable military operation forces who can implement normal military offense and contingency plans as required.
    - DOD must build and maintain viable cyber options and plans to control cyber conflict escalation and to shape the environment at all stages to minimize loss of life and destruction of property.

  • **Defense and Offense:**
    - DOD must be prepared to defend the United states and its interests against significant cyber-attacks if directed by the president and/or the secretary of defense to conduct CYBER operations against imminent or ongoing against the homeland.
    - DOD must also integrate the National guard and reserve units so they can support the regional governments where they are located.
    - DOD must provide defense support to civilian authorities upon request.

  • **Deterrence:** Department of Homeland Security (DHS) and DOD must prepare the defense of the US vital interests from disruptive and/or destructive cyber-attacks.
    - DHS must build and maintain robust alliances and partnerships to deter shared threats in local utilities, governments and private sectors to increase stability and security.
    - DOD and DHS must establish exchange programs with private sector to share cyber defense tools.

  • **Denial:** Federal Bureau of Investigation cyber division (FBICD) was to investigate, arrest and deter criminal activity in private sector as well as migrate the human threats from insider sabotage in government, financial and private cyber institutions.
    - **Response and Recovery:** Carnegie mellon CERT teams and Fema teams are to support civilian defense and disaster recovery responses to significant cyber attacks.

  • **Reconnaissance and Prevention:** DOD, and State Department were to build and maintain robust International alliances and partnership to deter threats while increasing the international cyber networks and stability.
The United States Cyber Command (USCYBERCOM) is a United States Armed Forces sub-unified command subordinate to United States Strategic Command. USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: defend Department of Defense information networks and; prepare to conduct "full spectrum military cyberspace operations" to ensure US/Allied freedom of action in cyberspace and deny the same to adversaries.\[20\]

Warning Most of the Cyber security cost are not reported, such as CIA, NSA, Military sub commands, In 2016, Market Research Media reported the listed budgets for civilian agencies was 28 Billion dollars which was larger than the reported budgets of almost all cyber involved counties in world. This is a low estimate since it does not include all civilian corporation costs on cyber security.
INITIAL MILITARY COMMANDS

2009:

United States

9th Army Signal Command houses:
Network Enterprise Technology Command (NETCOM)

UNITED STATES CYBER COMMAND
NATIONAL SECURITY AGENCY
UNITED STATES TENTH FLEET
THE 2017 MAJOR AGENCIES OF THE UNITED STATES ARE:

US CYBER SECURITY AGENCIES

- Office of the Cyber Security Coordinator
- Department of Homeland Security (DHS)
- National Security Agency (NSA)
- Cyber Command (CYBERCOM)
### WHAT US CIVILIAN GOVERNMENT IS SPENDING

<table>
<thead>
<tr>
<th>Number</th>
<th>Date of Creation</th>
<th>Years in Operation</th>
<th>Name</th>
<th>2016 Budget</th>
<th>2017 Budget</th>
<th>Number of Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1950</td>
<td>68</td>
<td>National Security Agency (NSA)</td>
<td>$</td>
<td>8</td>
<td>35,000</td>
</tr>
<tr>
<td>2</td>
<td>1953</td>
<td>65</td>
<td>CENTRAL Intelligence Agency (CIA)</td>
<td>$</td>
<td>15</td>
<td>21575</td>
</tr>
<tr>
<td>3</td>
<td>1958</td>
<td>60</td>
<td>(Defense advanced research projects agency (DARPA))</td>
<td>unknown</td>
<td></td>
<td>240</td>
</tr>
<tr>
<td>4</td>
<td>1988</td>
<td>30</td>
<td>Carnegie Mellem SEL_CERT (yearly non grant budget)</td>
<td>$</td>
<td>2</td>
<td>unknown</td>
</tr>
<tr>
<td>5</td>
<td>1993</td>
<td>25</td>
<td>Computer Emergency Readiness Team (CERT Teams)</td>
<td>unknown</td>
<td></td>
<td>CDA</td>
</tr>
<tr>
<td>6</td>
<td>2002</td>
<td>16</td>
<td>Federal Bureau of Investigation (FBI) (cyber division)</td>
<td>not reported</td>
<td>dynamic</td>
<td>dynamic</td>
</tr>
<tr>
<td>7</td>
<td>2009</td>
<td>9</td>
<td>Department of Homeland Security (DHS)</td>
<td>$</td>
<td>85</td>
<td>229000</td>
</tr>
<tr>
<td>a</td>
<td>2013</td>
<td>5</td>
<td>national Cyber security &amp; communications</td>
<td>dynamic</td>
<td></td>
<td>dynamic</td>
</tr>
<tr>
<td>b</td>
<td>1939</td>
<td>79</td>
<td>US coast guard (Assign to DHS when US not at war)</td>
<td>has two budgets</td>
<td></td>
<td>unknown</td>
</tr>
<tr>
<td>c</td>
<td>1978</td>
<td>40</td>
<td>FEMA Federal emergency management agency</td>
<td>$</td>
<td>14</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

Espionage and propaganda:  
- The budget is a low estimate because each has unpublished black budget as well.
- _$1,000,000,000 or 10 to the 9th power_ 

Emergency response:  
- Provides 35 billion in grants for in fracture harden.
- _$35 billion grants_

Criminal enforcement/deterrence:  
- 10 regions, 22 agency coordinated with state and local response teams

(yearly sub-total: _$159 billion_)

---

The table includes agencies involved in cyber security, excluding US industrial spending. Each entry provides the date of creation, years in operation, name of the agency, and budget information for 2016 and 2017. The agencies listed represent various aspects of cyber security, including espionage and propaganda, emergency response, and criminal enforcement/deterrence.
DHS DEPARTMENT OF HOMELAND SECURITY

CYBER DETERRENCE = TO PREVENT AN ENEMY FROM CONDUCTING FUTURE ATTACKS BY ATTACKING THEIR TECHNOLOGY
THE CIVILIAN AGENCIES OF THE US GOVERNMENT FOR CYBER SPACE ARE

FBI FOR CYBER CRIME AND COUNTER TERRORISM

• https://www.fbi.gov/investigate/cyber

• The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists. The threat is incredibly serious—and growing. Cyber intrusions are becoming more commonplace, more dangerous, and more sophisticated. Our nation’s critical infrastructure, including both private and public sector networks, are targeted by adversaries. American companies are targeted for trade secrets and other sensitive corporate data, and universities for their cutting-edge research and development. Citizens are targeted by fraudsters and identity thieves, and children are targeted by online predators. Just as the FBI transformed itself to better address the terrorist threat after the 9/11 attacks, it is undertaking a similar transformation to address the pervasive and evolving cyber threat. This means enhancing the Cyber Division’s investigative capacity to sharpen its focus on intrusions into government and private computer networks.

DARPA (CHASE) “CYBER HUNTING AT SCALE” PROJECT SOLICITATION

• To develop dynamic approaches to extract the right data at the right time from the right devices during an attack and disseminate protective measures dynamically. The price to be determined by bid unknown at this time.
THE CIVILIAN AGENCIES OF THE US GOVERNMENT FOR CYBER SPACE ARE:

Carnegie Mellon Software Engineering Institute (CERT)

- 5 year contract for 1.73 billion dollars with renewal option for an additional 5 years
- To provide to us industry for their software systems engineering and security
- Innovative technologies to meet the cybersecurity challenges

FEMA US Stafford Act

10 Regions, 22 agency coordinated with state and local response teams
NATIONAL SECURITY AGENCY (NSA) = CYBER ESPIONAGE = SURVEILLANCE
USCYBERCOM MILITARY RESPONSE
THE UNITED STATES CYBER COMMAND
US MILITARY CYBER EXPENDITURES APPROXIMATELY 10% OF IT BUDGET
US MILITARY CYBER EXPENDITURES
OF WHICH 50% GOES TO OPERATIONAL UNITS

DOD CYBER BUDGET DISTRIBUTION

MILITARY SERVICE DISTRIBUTION

Source: Defense Department
The Army Cyber Command (ARCYBER) is an Army component command for the U.S. Cyber Command. ARCYBER has the following components:

- Army Network Enterprise Technology Command / 9th Army Signal Command Started in 1918 restructured to cyber in 1998 20 years ago
- Portions of 1st Information Operations Command (Land)
- United States Army Intelligence and Security Command will be under the operational control of ARCYBER for cyber-related actions. Staff 10000 soldiers

Subordinate units, Cyber:

- Army Network Enterprise Technology Command
- Army Intelligence and Security Command (INSCOM) will be under the operational control of Army Cyber for cyber-related actions.
  - 1st Information Operations Command (Land) (1st IO CMD (L))
    - 1st Battalion - Trains and deploys field support, vulnerability assessment, and OPSEC awareness teams.
    - 2d Battalion - Conducts Army cyber opposing force operations at military training centers worldwide.
- 780th Military Intelligence Brigade (Cyber)
Air Force Cyber Command (Provisional) (AFCYBER (P)) was a proposed United States Air Force Major Command that existed only in provisional status. On 6 October 2008, the Air Force announced that the command would not be brought into permanent activation, and that the cyber mission would be transferred, with the standup of the Twenty-Fourth Air Force, to Air Force Space Command.

The Twenty-Fourth Air Force (24 AF) will be the United States Air Force component of United States Cyber Command (USCYBER). It has the following components:

- 67th Network Warfare Wing
- 688th Information Operations Wing
- 689th Combat Communications Wing
NAVY, MARINE CORP AND COAST GUARD (ATTACHED IN TIME OF WAR)

• Navy
  - The Navy Cyber Forces (CYBERFOR) is the type commander for the U.S. Navy’s global cyber workforce. The headquarters is located at Joint Expeditionary Base Little Creek-Fort Story. CYBERFOR provides forces and equipment in cryptology/signals intelligence, cyber, electronic warfare, information operations, intelligence, networks, and space. In September 2013, the United States Naval Academy will offer undergraduate students the opportunity to major in Cyber Operations.
  - Fleet Cyber Command is an operating force of the United States Navy responsible for the Navy’s cyber warfare programs. Tenth Fleet (established in 1940), 78 years ago is a force provider for Fleet Cyber Command. The fleet components are:
    • Naval Network Warfare Command
    • Navy Cyber Defense Operations Command
    • Naval Information Operation Commands
    • Combined Task Forces

• The Marine Corps Cyber Operations Group
  - MCCOG directs global Network Operations (NETOPS) and computer network defense of the Marine Corps Enterprise Network (MCEN) and to provide technical leadership in support of Marine and joint forces operating worldwide. The MCCOG is also responsible for intelligence gathering and analysis to develop future capabilities planning in accordance with DCO.
  - The MCCOG is the Computer Network Defense Service Provider (CNDSP) and serves as the Corps’ Global Network Operations and Security Center (GNOSC). The MCCOG provides 24/7 NETOPS C2 through its Operations Center. Under the OPCON (operational command) of MARFORCYBER, the MCCOG executes our Information NETOPS and DCO in support of our operational requirements in order to enhance freedom of action across all warfighting domains, while denying the efforts of adversaries to degrade or disrupt this advantage through cyberspace.
  - Key MCCOG tasks include:
    • operating and defending the MCEN
    • collecting and sharing DoDIN Situational Awareness
    • reporting and directing actions that proactively address threats and vulnerabilities
    • responding to operational incidents
    • providing technical leadership to ensure that our Corps and joint capabilities leverage new technologies to the advantage of the Marine warfighter
  - Marine Corps Cyberspace Warfare Group (MCCYWG)
• The Marine Corps Cyber Warfare Group

• MCCYWG is an administrative headquarters that organizes, trains, equips, provides administrative support, manages readiness of assigned forces, and recommends certification and presentation of Cyber Mission Force (CMF) Teams to U.S. Cyber Command.

• Key MCCYWG tasks include:
  • Conduct personnel management to organize and assign individuals to work roles and place them in work centers to ensure operational readiness of CMF Teams
  • Ensure all personnel are trained in accordance with USCYBERCOM Joint Cyberspace Training and Certification Standards and equipped to perform all duties and tasks outlined in the MARFORCYBER Mission Essential Task List (METL)
  • Advise COMMARFORCYBER on force employment considerations
  • Provide subject matter expertise for operational planning requirements

• Coast Guard Part of DHS rather than the Defense Department (DOD), the Coast Guard was the last uniformed service to stand up a service cyber component subordinate to USCYBERCOM in a direct-reporting capacity

• In 2013, the U.S. Coast Guard created a service-wide Cyber Command with a vision to achieve “a safe, secure and resilient cyber operating environment that allows for the execution of Coast Guard missions and maritime transportation interests of the United States.”

• They assessed what efforts would become part of the new command and what would remain within traditional Coast Guard units. All cybersecurity functions that were part of the Telecommunications and Systems Command or C4IT Service Center were added to CGCYBER missions to create a more holistic grouping of the service’s existing cybersecurity units, capabilities, and requirements.

• The service’s cyber mission is to: identify, protect against, enhance resiliency in the face of, and counter electromagnetic threats to the Coast Guard and maritime interests of the United States; provide cyber capabilities that foster excellence in the execution of Coast Guard operations; support Department of Homeland Security (DHS)
NAVY’S TEN FLEET COMPONENTS

- **Network operations & defense**
  - **CTF 1010 - NNWC**
    - CTG 1010.1 - NCTAMS LANT
    - CTG 1010.2 - NCTAMS PAC
    - CTG 1010.3 - NAVSOC
    - CTG 1010.6 - NCTS Naples
  - **CTF 1020 - CO NCDOC**
    - CTG 1020.1 - NCDOC
    - CTG 1020.2 - NIOC Pensacola

- **Information operations**
  - **CTF 1030 - CO NIOC Norfolk**
    - CTG 1030.1 - NIOC Norfolk
    - CTG 1030.2 - NIOC San Diego
    - CTG 1030.3 - NIOC Whidbey Island

- **Research and development**
  - **CTF 1090 - CO NCWDG**
NAVY’S TEN FLEET COMPONENTS

- Service cryptologic component operations
  - CTF 1000 - C10F
    - CTG 1000.1 - NIOC Menwith Hill Station
    - CTG 1000.2 - NIOC Sugar Grove
    - CTG 1000.3 - NIOC Misawa
    - CTG 1000.4 - NIOC Texas
    - CTG 1000.5 - NIOC Georgia
    - CTG 1000.6 - CWG-6 (formerly NIOC Maryland)
    - CTG 1000.7 - NIOC Hawaii
    - CTG 1000.8 - NIOC Colorado
    - CTG 1000.9 - NIOD Yakima
    - CTG 1000.10 - NIOD Alice Springs

- Fleet and theater operations
  - CTF 1040 - CO NIOC Texas
    - CTG 1040.1 - NIOC Texas
  - CTF 1050 - CO NIOC Georgia
    - CTG 1050.1 - NIOC Georgia
    - CTG 1050.2 - NIOC Bahrain
  - CTF 1060 - CO CWG-6
    - CTG 1060.1 - CWMA-61
    - CTG 1060.2 - FIOC UK
  - CTF 1070 - CO NIOC Hawaii
    - CTG 1070.1 - NIOC Hawaii
    - CTG 1070.2 - NIOC Yokosuka
    - CTG 1070.3 - NIOC Misawa
  - CTF 1080 - CO NIOC Colorado
    - CTG 1080.1 - NIOC Colorado
RUSSIA

- **Cyberwarfare by Russia** includes denial of service attacks, hacker attacks, dissemination of disinformation and propaganda, participation of state-sponsored teams in political blogs, internet surveillance using SORM technology, persecution of cyber-dissidents and other active measures. According to investigative journalist Andrei Soldatov, Russia thinks cyber warfare is just traditional propaganda in a new medium cyber space. Previously they controlled the press, radio and television and the dramatic arts, now they are trying to control the world wide web.

- some of these activities have been coordinated by the Russian signals intelligence, which is part of the FSB and was formerly a part of the 16th KGB department, Russia employs cyberwarriors within its military and intelligence services. Indeed, the cyberespionage groups dubbed APT28 (aka Fancy Bear) and APT29 (aka Cozy Bear and The Dukes) are believed to correspond to Russia’s military intelligence agency GRU and its state security organization FSB, respectively. Both groups have been implicated in hundreds of cyberoperations over the past decade, including U.S. election hacking.

- An analysis by the Defense Intelligence Agency in 2017 outlines Russia’s view of “Information Confrontation” or IPb (informatsionnoye protivoborstvo) as “strategically decisive and critically important to control its domestic populace and influence adversary states”, delineating the term ‘Information Confrontation’ into two categories of ”Informational-Technical” and ”Informational-Psychological” Effects.

- The former encompasses network operations relating to defense, attack, and exploitation with the latter relating to ”attempts to change people’s behavior or beliefs(i.e. social networks) in favor of Russian governmental objectives. 
China

38 “According to reports, a classified FBI account states that the People’s Liberation Army of China has developed a cadre of 30,000 cyberspies who are supplemented by more than 150,000 “private sector” cyber experts “whose mission is to steal American military technological secrets and cause mischief in government and financial services.”

• PLA unit 61398