2013

DISEC 2013
Background Guide

MIT Model United Nations Conference V

disec2013@mitmunc.org

Topic 1:

Usage of Unconventional Weaponry

Introduction

Conventional warfare is a form of warfare conducted by using conventional military weapons and battlefield tactics between two or more states in open confrontation. The forces on each side are well-defined, and fight using weapons that primarily target the opposing army. It is normally fought using conventional weapons, and not with chemical, biological, or nuclear weapons. Unconventional warfare, on the other hand, uses unconventional weapons. It targets civilian populations as well as armed forces, and specializes in unconventional tactics.

Despite numerous efforts to reduce or eliminate them, many nations continue to research and/or stockpile chemical weapon agents. Most states have joined the Chemical Weapons Convention, which outlaws the production, stockpiling or use of chemical weapons. The agreement is administered by the Organisation for the Prohibition of Chemical Weapons (OPCW).

The Biological Weapons Convention (1972) is an international treaty banning the use or stockpiling of bio-agents; it currently has 165 state signatories. Bio-agents are, however, widely studied for defensive purposes under various biosafety levels and within biocontainment facilities throughout the world. In 2008, according to a U.S. Congressional Research Service report, China, Cuba, Egypt, Iran, Israel, North Korea, Russia, Syria and Taiwan were considered, with varying degrees of certainty, to be maintaining bio-agents in an offensive biological weapon program capacity.

Debate Format

The resolution to this issue should take the form of a treaty. In a treaty, preambulatory clauses are used in opening, followed by chapters divided into articles, with Article 1 defining all related terms and the last article including the signatures of all countries in agreement prior to an agreed upon deadline. A sample can be found in the sources, as an arms trade treaty was written by the Disarmament Committee of Robert College International Model United Nations (RCIMUN) in 2010. (http://www.rcimun.org/post2010/report%20book.pdf)

Documented Attacks

As of December 2004, Israel has signed but not ratified the Chemical Weapons Convention, and according to the Russian Federation Foreign Intelligence Service, Israel has significant stores of chemical weapons of its own manufacture. It possesses a highly developed chemical and petrochemical industry, skilled specialists, and stocks of source material, and is capable of producing several nerve, blister and incapacitating agents. Various accounts of Palestinians being subject to attacks of chemical agents have appeared since, especially in 2012.

In addition, there has been great concern the existence and use of chemical and biological agents in Syria, as the Secretary General conveyed those concerns in writing to President Assad some months ago and has done so again in a letter handed over to the Syrian authorities December 4th. NBC News reports that the Syrian military is prepared to use chemical weapons against its own people and is awaiting final orders from President Bashar Assad. The military has loaded the precursor chemicals for sarin, a deadly nerve gas, into aerial bombs that could be dropped onto the Syrian people from dozens of fighter-bombers.

Countries Involved

Syria

Syria is not a signatory of the Chemical Weapons Convention or the Comprehensive Test Ban Treaty. It is believed Syria first received chemical weapons in 1973 from Egypt in the form of artillery shells. Since then it is thought Syria has one of the most advanced chemical weapons programs in the Middle East.

Israel

Israel is believed to have developed an offensive biological warfare capability. The US Congress Office of Technology Assessment records Israel as a country possessing a long-term, undeclared biological warfare program. Israel is not a signatory to the Biological Weapons Convention. In addition, Israel has signed but not ratified the Chemical Weapons Convention. There are speculations that a chemical weapons program might be located at the Israel Institute for Biological Research (IIBR) in Ness Ziona.

US Congress Office of Technology

Assessment has recorded Israel as a country generally reported as having undeclared chemical warfare capabilities, and an offensive biological warfare program. Officially Israel neither confirms nor denies possessing nuclear weapons.

USA

The U.S. policy on the use of chemical weapons is to reserve the right to retaliate. First use, or preemptive use, is a violation of stated policy. Only the president of the United States can authorize the first retaliatory use.

North Korea

North Korea is not a signatory of the Chemical Weapons Convention and has never officially acknowledged the exsitence of its offensive CW program. Nevertheless, the country is believed to possess a substantial arsenal of chemical weapons. It reportedly acquired the technology necessary to produce tabun and mustard gas as early as the 1950s.

Sources and Further Reading

Chemical Weapons Convention
http://www.opcw.org/chemical-weapons-convention/

Biological Weapons Convention
http://www.unog.ch/80256EE600585943/(httpPages)/04FBBDD6315AC720C1257180004B1B2F?OpenDocument

Organization for the Prohibition of Chemical Weapons
http://www.opcw.org/

The Biological Weapons and Toxins Convention Site
http://www.opbw.org/

UN's Biological Weapons Convention Page
http://www.un.org/disarmament/WMD/Bio/

The Seventh BWC Review Conference Briefing Book
http://www.bwc2011.info/

RCIMUN 2010 Report Book including a sample of a treaty resolution
http://www.rcimun.org/post2010/report%20book.pdf

Topic 2:

The Growing Threat of Cyber-Terrorism and Cyber-Warfare

Description

Given the recent leaps in technological developments and the increasing reliance, worldwide, of both governments and individuals on digital means of accessing, storing, and manipulating data, it has become crucial to address the issues of cyber-terrorism and cyber-warfare. There is currently no universal definition for cyber-warfare, and one aspect of addressing this challenge lies in the difficulty of finding formal boundaries for this type of warfare.

The Congressional Report on Cyber-Terrorism defines the term as "the politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies". Further, based on the Department of Defense operations for information warfare, the definition maybe extended to include physical attacks on computer facilities and transmission lines.

The International Telecommunication Union, under the United Nations, defines the term as "unlawful attacks and threats of attack against computers, networks, and stored information to intimidate or coerce a government or its people in furtherance of specific political or social objectives", further specifying that "cyber-terrorism", in combining aspects of both terrorism and cyber-crime, is not a new branch of criminal activity, but rather a term coined to describe new aspects of an already defined area.

It is vital, then, when facing the issue of cyber-terrorism and cyber-warfare, to accurately define the terms and boundaries within which one will be operating. The intent, means and effect of these attacks should be defined in a manner distinct from other forms of cyber-crime as well as more traditional means of terrorism.

Documented Attacks

The rise of technology as a means of communication and information storage is relatively recent, and cyber-terrorism rose to public attention around the late 1980s. The Millennium Bug, or the Year 2000 problem, while not strictly an act of cyber terrorism, served to fully illustrate society's newfound dependence on computers and computer networks and highlighted the extent of devastation such an attack had the potential to cause.

Currently the largest recorded instances of cyber terrorism include 'Titan Rain', the name designated by United States government for a series of attacks on government infrastructure beginning in 2003, including the Department of Defense and NASA, designed to obtain information and disrupt computer networks. These attackers, while rumored to be Chinese in origin, have been able to obscure their digital train through proxies, viruses and other means, and remain unknown.

In 2007, a variety of Estonian organizations were targeted in a large-scale

series of cyber-attacks which coincided with the then government's dispute with Russia. The attack caused tension between the Estonian government and Russian authorities but due to the difficulty in tracing its origins, it was never fully attributed to any one organization. 'Operation Aurora' was an attack on Google in 2009, among other large organizations, to infiltrate and steal intellectual property. The attack targeted Google servers, and it was suggested that the hackers, purportedly originating from China, were accessing Gmail databases to look for communications between Chinese dissidents.

The attack on Saudi Armaco, the Saudi Arabian petroleum enterprise, succeeded in infecting 30,000 computers and is possibly the most severe attack in recent history. Though there have certainly been similar threats of a physical nature, the danger of this cyber-attack was that it was completely unprecedented and unexpected; the intangible nature of the threat made it difficult to respond to.

These attacks serve to illustrate that the full extent and range of cyber warfare has not been explored, and that the capabilities of attackers extend to the disruption of government networks, the theft of intellectual property and government intelligence, the infiltration of vital infrastructures (with regard to national security, defense, and economic safety, among others), as well as myriad other aspects which are certainly not fully documented.

Pre-existing Action

UNODC: The use of the Internet for terrorist purposes
http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
This document emphasizes the need for international cooperation as well as collaboration between justice systems and the private sector in the process of combating cyber-terrorism. It urges member nations to join existing international conventions on terrorism, as well as to implement General Assembly and Security Council resolutions. Further, it suggests the establishment of clear national policies criminalizing unlawful activity on the internet, empowering law-enforcement agencies to investigate and act in defense of these policies, regulating internet-related services and developing specialized judicial procedures with regard to aforementioned policies.

UN CTITF: Countering the Use of the Internet for Terrorist Purposes
http://www.un.org/en/terrorism/ctitf/pdfs/WG_Compendium-Legal_and_Technical_Aspects_2011.pdf
This document urges the establishment of legal provisions to support and enhance technical solutions to terrorist activities over the internet. Cyber-crime specific legislation has become necessary, as using traditional means to address cyber issues has become inadequate in the face of the rapidly expanding digital world. It specifies that there is not a common approach to cyber-crime, and each solution must be flexible enough to address the multifaceted nature of such terrorist activity.

Council of Europe: Convention on Cybercrime
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
The Budapest convention on cybercrime is one of the first international treaties specifically addressing computer and Internet crimes. It approaches the subject on multiple fronts, suggesting the synchronization of national and international laws, urging international cooperation and improving investigative techniques with regard to cyber-crime. In terms of legislature, it stresses the necessity of precise laws directed specifically at crimes committed through or in relation to computers and computer systems, as well as providing the means for governments and judicial bodies to enforce and prosecute said laws.

Challenges/Problems

Cyber warfare is difficult to address in that it has a variety of facets that must be covered. The definition and bounds of what the term 'cyber-terrorism' addresses will determine the extent that legislative means will be able to equip agencies. Currently, both infrastructure and statutes remain inadequate. The attacks themselves are difficult to source, and the anonymity of the internet allows groups to act while hidden behind proxies; this difficulty, as illustrated in the Estonian attacks, gives governments and official agencies the freedom to finance, support or otherwise encourage activities while remaining officially distanced from the events.

We've addressed the various definitions of cyber-warfare in the previous section, but it is valuable to note that the definition itself, while seemingly a small aspect, is vital when it comes to actively defending against such attacks. The jurisdiction of legislature can only extend to areas that are laid out in concrete terms, and without these terms the ability to address such attacks is greatly hindered.

The current statutory infrastructure relies heavily on the Federal Information Security Management Act, which provides some means to establish agency-level defenses, which addresses assessment of risk and provides a framework for implementing defenses, but remains clumsy and inefficient for national governments, as well as lacking a focus on operational security.

Further, the physical aspect of cyber terrorism is not to be dismissed. Attacking the facilities and transmission lines of systems that support computer infrastructures would certainly cripple agencies that rely on said infrastructures for operations. The use of cybernetic means to further physical acts of terrorism, through recruiting members, coordinating movements and other communications is also a distinct danger.

Ultimately, one of the most pressing issues is that the digital realm is developing faster than current security measures can be adapted, and the infinitely flexible nature of the internet allows attackers to rapidly and creatively outmaneuver policies and defense mechanisms that remain clunky and slow. A related difficulty in addressing cyber warfare lies in its indefinability and constant growth, as well as the lack of a framework that reliably addresses the issues of threat detection, response and prevention.

Countries Involved

United States

The United States is currently at the forefront of technological development and has subjected to multiple cyber-attacks. The framework and legislature in place is currently highly inadequate, and the United States has been unable to trace many of the attacks, despite suspicions regarding the origins.

Saudi Arabia

Saudi Arabia was the victim of the most recent instance of cyber-terrorism, but has a history of suffering from a plethora of terrorist attacks, some of which have been claimed by Al-Qaeda. Cyber security experts are addressing the issue, and Prince Sultan has stressed the need for immediate, effective action against the terrorist groups that employ these techniques.

Iran

Multiple attacks against the United States, as well as the recent Aramco incidents, have been attributed to Iran. The government is suspected of targeting United States banks, and companies, utilizing this new frontier to their advantage. However, it is difficult to truly trace the origin of these attacks.

China

Several of the largest acts of cyber warfare in the last 20 years have been attributed to China, and, while not government-sponsored, they do highlight the need for stronger cyber-crime prevention and defense in the nation. While China does currently employ an online defense unit, the "Blue Army", there have been concerns that this team may have been used offensively against foreign governments.

Sources and Further Reading

International Telecommunications Union Global Strategic Report on Cybersecurity
http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/global_strategic_report.pdf

International Telecommunications Union Cybersecurity Forum
http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf

Congressional Research Service Report: Computer Attack and Cyber Terrorism
http://www.fas.org/irp/crs/RL32114.pdf

Critical Infrastructures: Background, Policy, and Implementation
http://www.fas.org/sgp/crs/homesec/RL30153.pdf

Terrorist Capabilities for Cyberattack: Overview and Policy Issues
http://www.fas.org/sgp/crs/terror/RL33123.pdf

Federal Information Security Management Act of 2002
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

CSIS Commission Report on Cybersecurity for the 44th Presidency
http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

UN Department on New Challenges and Threats: Cybercrime, New Threat and Global Response
http://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/Russia_1_Cybercrime_EGMJan2011.pdf