



**MALMÖ HÖGSKOLA**  
**Teknik och Samhälle**

# **”CYBERWAR - det virtuella kriget”**

EN LITTERATURANALYS OM CYBERWAR

***Av: Almin Jusufovic***

Examensarbete i datavetenskap

15 HP

Datavetenskap

Juni 2014

Malmö högskola

Teknik och Samhälle

202 50 Malmö

***Handledare: Bengt J Nilsson, Malmö Högskola***

***Extern Hanledare: Ross Tsagalidis, Svenska Försvarsmakten***

# **”CYBERWAR - det virtuella kriget”**

Titel: ”Cyberwar – det virtuella kriget.”

Författare: Almin Jusufovic

Malmö: Malmö Högskola, Teknik och Samhälle, Datavetenskap (2014)

**Sammanfattning:** Syftet med denna uppsats är bland annat att utforska begreppet cyber-war. Cyber-attacker utgör stora hot mot infrastrukturen, datorstyrda system och nätverksbaserade tjänster, enligt tidigare forskning. Men hur hotfulla är dessa attacker egentligen? Ska vi frukta att framtida krig blir virtuella? Kan en ond grupp av människor med några rader av kod få kontroll över vår nation? För att få en bättre förståelse och för att kunna svara på frågorna, har jag med hjälp av tidigare publicerade publikationer gjort en litteraturanlys. Analysen bygger på sammanställning och jämförelse av åtta olika publikationer. Enligt forskningen så tyder tecken på att cyber-war kan vara ett framtida hot.

*Nyckelord:* Cyber-war, Cyber-threat, Cyber-attack, Cyber-terrorism

## **Abstract**

The purpose of this paper is to explore the concept of cyber-war. Cyber-attacks pose major threats to infrastructure, computer systems and network-based services, according to previous research. But how threatening are these attacks? Should we fear that future wars will be virtual? Can a group of people with a few lines of code get control of our nation? To get a better understanding and be able to answer these questions, I have used previously published publications and have made a literature analysis. The analysis is based on a compilation and comparison of eight different publications. According to the research, cyber-war may be a future threat.

## **Förord**

Att skriva en kandidatuppsats kräver stöd och vägledning från många håll. Det har stundtals varit svårt. Jag fastnade vid vissa tillfällen och tack vare intressanta och givande diskussioner med mina handledare fick jag nya infallsvinklar. Under arbetsgången har jag fått assistans och inspiration av min handledare *Bengt J Nilsson – Malmö Högskola, Svenska Försvarsmakten* och min externa handledare *Ross W Tsagalidis – Svenska Försvarsmakten*.

Ett stort tack till alla!

# Innehållsförteckning

1. Inledning .....	6
2. Begreppsdefinitioner.....	7
2.1 Vad är en cyber-attack? .....	7
2.2 Vad är cyber-hot? .....	7
2.3 Vad är ett cyber-krig? .....	7
2.4 Vad är en hackare?.....	8
3. Frågeställning.....	9
3.1 Avgränsning.....	9
4. Metod .....	9
4.1 Metoddiskussion .....	9
5. Bakgrund.....	10
5.1 Historisk överblick.....	10
5.2 Hotbilder .....	15
6. Artiklar.....	19
6.1 Artikel A).....	19
6.2 Artikel B) .....	21
6.3 Artikel C) .....	22
6.4 Artikel D).....	23
6.5 Artikel E) .....	24
6.6 Artikel F).....	25
6.7 Artikel G).....	26
6.8 Artikel H) .....	27
7. Jämförelse av material .....	28
8. Diskussion.....	33
9. Slutsats .....	34
10. Referenser .....	35

# 1. INLEDNING

Teknologin har ett stort inflytande på våra liv idag. Vi använder oss av smarta telefoner som pratar med oss, bilar som parkerar av sig själva och våra internetsökningar går främst via världens mest kända sökmotor, Google [28, 29]. Vårt användande av teknologin förändras i snabb takt. Många människor skulle inte kunna tänka sig ett liv utan de teknikföremål som vi använder oss av idag [30, 31].

I samma takt som teknologins utveckling har tagit fart, har även automatiseringen av system uppkommit. Varför har automatisering uppkommit? Dels för att det är billigare, går mycket fortare och maskiner kan vara igång dygnet runt och dels för innovationens skull. Banksystemet till exempel består av flera olika datorsystem som är sammankopplade, för att vår kommersiella värld ska fungera väl. För att samhället skall kunna fortsätta utvecklas i samma takt som det har gjort hittills. Vårt elsystem drivs av gigantiska generatorer som genererar så mycket energi att de klarar av att förse städer med el. Även dessa system är till viss del datorstyrda och automatiserade [82, 83].

Det finns en påtaglig rädsla för att någon ska kunna slå ut dessa komplexa system [84, 85]. Detta skulle kunna hota ett lands välstånd, och slå ut delar av infrastrukturen som utgör ett påtagligt hot mot medborgarna. Andra anser att allt som har med cyber-war att göra är förstorat. Att det därmed inte finns någon som helst anledning, till att vi ska behöva oroa oss över att någon en dag ska förstöra allt genom en cyber-attack [1,2].

Människor har idag skaffat sig vanor som de har blivit bekväma med [86, 87, 88]. Några frågor som vi sällan ställer oss men bör tänka på är; ”Hur stora är cyber-hoten mot våra samhällen?”, ”Hade vi klarat av en cyber-attack mot några av våra system och hur hade det påverkat vårt vardagsliv?”, ”Kan stora organiserade grupper slå ut vårt banksystem?”

Samhället idag följer teknologins utveckling och allt fler människor använder sig av teknikens innovationer [79, 80, 81]. Innovationer som har blivit en del av vår vardag. Ju fler innovationer desto fler ställen blir vi sårbara på. Med detta är cyber-war ett mycket intressant och allt mer aktuellt område för framtiden.

## **2. Begreppsdefinitioner**

### **2.1 Vad är en cyber-attack?**

Cyber-attack innebär att man angriper en dator eller ett datorstyrt system med hjälp av internet. Ett nätverk som man använder sig av för att obemärkt kunna erhålla kontroll över en viss dator eller system [10,11,12,14].

En cyber-attack utförs för att skada, störa eller överbelasta ett system. Det finns attacker som kan orsaka skador om hemlig information hamnar i fel händer och/eller läcker ut till allmänheten. Som ett exempel kan en så kallad ”hackare” ta sig in i ett system enbart för att bevisa att dess säkerhet är dålig. Det kan anses som en varningsklocka eller ett stort hot, beroende på dess utdragna fakta. Åtgärden blir då att man arbetar för att säkra systemet ytterligare.

Till skillnad från en hackare, har vi organiserad brottslighet som samlar information på nätet för att kunna komma åt stora summor av pengar så att man kan finansiera sina brott. Sedan finns det även terrorister som utför sina cyber-attacker enbart för att skada ett lands infrastruktur eller ekonomi [10,11,12,14].

### **2.2 Vad är cyber-hot?**

Cyber-hot innebär hot där antingen ett datorsystem eller ett nätverkssystem blir utsatt för olaga intrång. Om ett företag anlitar en ”White-hat” hackare, just för att denne ska kunna utföra en attack i syfte att hitta svagheter i deras system. Då anses det inte vara ett direkt hot. Då detta utförs av företaget själv, för att kunna säkra dess system ytterligare.

Men om samma hackare skulle ta sig in i samma system utan företagets vetskap, för att komma åt hemlig information eller för att överbelasta systemet. Då anses det vara ett allvarligt hot. Eftersom att man begår ett brott då man gör ett intrång i företagets system [15]

### **2.3 Vad är ett cyber-war?**

Det finns ett flertal olika sätt att föra krig, det är inte bara på traditionellt sätt som krig utförs. Så som, där människor slåss och använder sig av diverse vapen till lands, till havs där man använder sig av avancerade båtar och i luften där man använder sig av krigsflygplan.

Det finns även krig i den virtuella världen. Ett cyber-war är ett avancerat sätt för länder och olika folkgrupper att föra kriga i en virtuell värld. Det är en värld där man använder sig av datorer och internet för att kunna utföra virtuella attacker. Attacker som resulterar i att man ostört kan sprida sin propaganda, spionera eller samla på sig hemlig information. Att obemärkt utföra en attack beror delvis på hur pass smidigt man utför attacken men även hur avancerad säkerhet den utsatta har [16,17,18,19].

## 2.4 Vad är en hackare?

En hackare är en person som lyckas bryta sig in i ett nätverkssystem eller datorsystem, ett system som sägs vara säkert. Att vara hackare behöver nödvändigtvis inte vara något negativt.

Det finns två typer av hackare, ”White-hat” och ”Black-hat”. En ”White-hat” hackare är en person som jobbar på ett företag och bidrar med sina färdigheter för att öka säkerheten i systemen. En ”Black-hat” hackare är en person som på olagligt sätt bryter sig in i ett system för att antingen stjäla information, eller för att skryta om sina färdigheter [20,21].

### 3. Frågeställning

Min övergripande frågeställning är:

- *Är cyber-war verkligen ett hot mot våra samhällsfunktioner?*

#### 3.1 Avgränsning

För att göra uppsatsen och forskningsfrågan tydlig och hanterbar har jag valt att göra vissa nödvändiga avgränsningar. Först och främst kommer jag att behandla en stor del av ämnet för att läsaren ska få en bra överblick och bättre förståelse. Uppsatsens syfte är dock att fokusera på attacker som kan orsaka kostsamma respektive dödliga skador. Med detta menar jag att jag i huvudsak kommer att skriva om kampen mellan statsmakter och dess jakt på effektiva cyber-attacker vars syfte är att förstöra säkra samhällssystem.

### 4. Metod

Denna uppsats bygger på en kvalitativ litteraturstudie av 8 artiklar. Det innebär en sammanställning och kritiskt granskning av dessa. Anledningen till att jag valde just dessa artiklar är för att de innehåller relevant fakta som hjälper till att besvara min forskningsfråga. Valet av nyckelorden (Cyber-war, Cyber-threat, Cyber-attack, Cyber-terrorism) gjordes utifrån min forskningsfråga. Nyckelorden möjliggjorde en begränsad sökning via Malmö högskolans sökmotor, Summon. Jag valde även att ta med nyare tidningsartiklar som behandlar ämnet cyber-war eftersom det inte finns nyare vetenskapliga texter som bearbetar mitt valda ämne. Konkret har jag studerat artiklarna och gjort en jämförelse av materialet för att kunna besvara min fråga om cyber-war. Ifall det kan anses vara ett verkligt hot eller kanske rent av är ett förstorat ämne som får mycket uppmärksamhet utan en saklig grund.

#### 4.1 Metoddiskussion

Det finns relativt lite forskningsmaterial inom mitt ämne som är av ny karaktär, vilket är något av en nackdel för min studie. Därför har det varit svårt att få fram relevant data till min analys. Hur som helst var det inte omöjligt och utifrån en rad forskningsartiklar som behandlar området, har jag lyckats få både bredd och djup för att kunna utföra min studie. Jag har valt en kvalitativ metodansats vilket även stöds av Trost (2005), som menar på att kvalitativ metodansats är adekvat när det handlar om att försöka förstå och hitta mönster inom ett problemområde. Man skulle också kunna använt sig av intervjuer, för att på så sätt kunna analysera och tolka data Trost (2005), som sedan utgör ett underlag till forskningsfrågan. Jag anser dock att mitt val av tillvägagångssätt är mycket väl anpassad, då den belyser olika perspektiv och bygger på befintlig forskning inom området.

## 5. BAKGRUND

### 5.1 Historisk överblick

När Sovjetunionens satellit, Sputnik, skickades upp i rymden. Kände sig USA underlägsna inom teknologin. Då började den stora forskningen efter det som vi idag kallar för Internet. Det startade som ett experiment av USAs försvarsdepartement. För att länka ihop försvarsdepartementet med militära forskningsföretag. Men även med universitet som höll på med forskning. Det var början på ett nät som kallades ARPANET (*ARPA står för Advanced Research Projects Agency*) [39, 40, 41, 42, 43, 44, 45]. Syftet med detta var att skapa en militär kommunikationskanal, som inte var beroende av endast en datorcentral, som vid en fysisk attack kunde slås ut. Arpanätets huvudsakliga uppgift, var att på ett säkert sätt kunna leverera information, som skickades över nätet. Till en början var det enbart några universitet och militären som var ihop länkade till ARPANET. När detta sedan presenterades för allmänheten, växte nätverket och fler universitet anslöt sig. Vilket var en stor framgång. År 1975 lämnades nätverket över till Department Of Defense. Som bestämde sig för en delning av ARPANET. Nätverket delades upp till ett nytt ARPANET och MILNET. Det nya ARPANET var för den icke militära delen, medan MILNET tjänade militären. På så sätt kunde man hålla hemlig information borta från allmänheten.

I början av 1983 gick man över från NCP (Network Control Protocol) till det som används än idag TCP/IP (Transmission Control Protocol). Det var vid denna övergång som vilket nätverk som helst världen över kunde ansluta sig till ARPANET [39, 40, 41, 42, 43, 44, 45].

Allt fler privatpersoner, men även företag började ansluta sig till nätverket och det fortsatte att växa. På grund av tillväxten så delade man upp nätverket i flera olika delar, så att man genom global adressering kunde skilja på det.

Strax efter ARPANET började attackerna att ta form. Nedan följer en lista på uppmärksammade attacker samt olaga intrång som började redan år 1982 [101, 102]:

**1982** *After learning that the Soviet Union planned to steal software from a Canadian company to control its Trans-Siberian Pipeline, the CIA alters the software to cause the pipeline to explode. It is considered the first cyberattack.*

**1986** *Over the course of 10 months beginning in August, Clifford Stoll, a physics researcher at the University of California at Berkeley, tracks down a hacker who had broken into computers at the Lawrence Berkeley National Laboratory, a U.S. Department of Energy facility, and other military computers in the U.S. He traced the hacker to Germany. It is the first such investigation.*

**1988** *An Internet worm temporarily shuts down about 10% of the world's Internet servers. It is the first occurrence of an Internet worm. Robert Tappan Morris, a student at Cornell University, released the worm. Morris is the first person tried and convicted under the computer fraud and abuse act.*

**1990** *Arpanet becomes the operational network known as the Internet, with about 2.6 million people around the globe connected.*

**1994** *Computers at the Rome Air Development Center at Griffiss Air Force Base in New York are attacked 150 times by anonymous hackers, who use a "sniffer" program to steal login credentials and sensitive information from the lab, which conducts research on artificial intelligence systems, radar guidance systems, and target detection and tracking systems. The hackers then use the login information to access the computers of other military and government facilities, including NASA's Goddard Space Flight Center and the Wright-Patterson Air Force Base.*

**1997** *The NSA conducts a test, known as Eligible Receiver, to assess the vulnerability of government and military computers to a cyberattack. The exercise reveals that systems throughout the country could be hacked and disrupted with relative ease using commercial computers and software.*

**1998** *Analysts with the Air Force Computer Emergency Response Team in San Antonio, Texas, notice intrusions into their computer networks from several academic institutions, including Harvard. The hackers, who turned out to be three teenagers, exploited a weakness in the network's operating system. The event is a wake-up call to the government and prompted President Bill Clinton to develop a cyber-security plan.*

**2000** *NIST chooses the Advanced Encryption Standard (AES) for classified information; it's formally approved in 2001.*

*The ILOVEYOU worm, a.k.a. love bug, infects government and private systems worldwide. In response, U.S. pushes for the Council of Europe Cybercrime Treaty, to harmonize computer crime laws among nations.*

**2001** *The worm named Code Red affects computer networks running a Microsoft operating system. Some websites, including the White House site, are disabled.*

**2003** *Anonymous, the group of hackers who refer to themselves as "Internet activists" and attack government, corporate, and religious websites, is organized. While the group avoids adhering to a strict philosophy, its members seem united in their opposition to censorship.*

*President George Bush announces the creation of a new office under the Department of Homeland Security, the National CyberSecurity Division, and lays out a National Strategy to Secure Cyberspace to protect the nation's computer and information systems from a cyberattack.*

*Hackers, believed by U.S. officials to be backed by the Chinese military, search to find vulnerable computers in the military's computer network and steal sensitive information. The attacks continued for about three years and were given the name Titan Rain by U.S. officials.*

**2006** *NASA begins to block emails with attachments to prior to the launch of space shuttles to prevent hackers from sabotaging launch plans by gaining unauthorized access to the agency's computer network.*

**2007** *Estonia's government websites are hacked by distributed-denial-of-service-attacks and are compromised for 22 days. The hackers are believed to be backed by the Russian government. Targets include the president's office, Parliament, law enforcement officials, and Estonia's two biggest banks.*

*The email account of U.S. Secretary of Defense Robert Gates is hacked. Officials blame China's People's Liberation Army.*

*British government officials announce that hackers have breached the computers of the Foreign Office and other government agencies. The hackers are believed to be members of China's People's Liberation Army.*

**2008** *An employee at the U.S. Central Command put a flash drive into a laptop and accidentally unleashed "Operation Buckshot Yankee," the worst breach of U.S. computers to date, exposing data on classified and unclassified systems. The fact that it was a fairly unsophisticated worm — placed by a foreign intelligence agency — made the breach more alarming. It prompted the Defense Department to completely remake its cyber defense strategy, parts of which were declassified in 2010. "It isn't the most capable threat, but that's the point," then-Deputy Defense Secretary William Lynn said at the time, "... We need a new strategic approach."*

*In the weeks before the war between Russia and Georgia, Georgia is hit by distributed-denial-of-service-attacks and many of the government's computer networks are disabled, including that of President Mikheil*

*Saakashvili. Media and transportation companies are also affected. Georgian officials accused Russia of launching the attack.*

*Pentagon officials discover that a flash drive containing a covert program was inserted into a laptop at a base in the Middle East. The program collected data from a classified Department of Defense computer network and transferred it to computers overseas. Government officials say the hack was carried out by a foreign intelligence agency and called the intrusion, "most significant breach of US military computers ever."*

**2009** *The Aurora attacks, reportedly originating in China, hit Google and 33 other companies in search of intellectual property. In subsequent years, security experts report the well-funded group continues to strike defense-related and other industries.*

*Israel's government Internet sites are attacked during the conflict with Hamas in the Gaza Strip. Government computers are barraged with as many as 15 million junk emails per second, and the computers are temporarily paralyzed. Israel suspects Hamas financed the hack.*

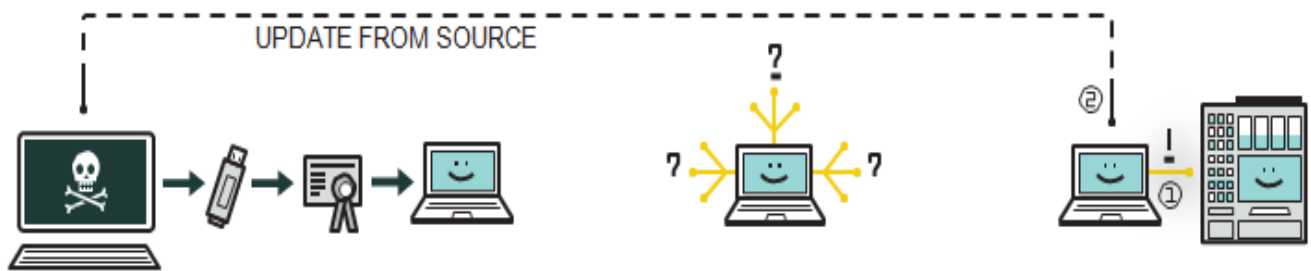
*Canadian researchers at the Munk Center for International Studies at the University of Toronto, announce that hackers based in China had penetrated almost 1,300 computers in 103 countries, including those belonging to embassies, government offices, and the Dalai Lama, and stole documents and other information.*

*News reports say that Iraqi insurgents had hacked into live feeds being sent by U.S. drones to military officials on the ground.*

Redan i tidigt skede ser man att det förekom virus/cyberattacker. Det lär inte bli bättre ifall det fortsätter i samma takt eftersom dem flesta system idag är uppkopplade mot nätet. Ett annat exempel på en attack, var det sofistikerade viruset *Stuxnet*. Som slog ut Irans nukleära turbiner, genom att lura systemet och ändra dess värden utan att det upptäcktes och därmed förhindrade processen av framtagandet för kärnvapen. Ett listigt dock väldigt effektivt sätt att sabotera samtidigt skada ett projekt som tog år att utveckla.

Nedanstående bild visar och förklarar hur USA tillsammans med Israel utförde en attack med det så kalla viruset STUXNET [75, 76, 77].

## Hur Stuxnet fungerade:



### 1. INFECTION

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

### 2. SEARCH

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

### 3. UPDATE

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



### 4. COMPROMISE

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.



### 5. CONTROL

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



### 6. DECEIVE AND DESTROY

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

*(Bild 1, bilden är hämtad från IEEE Spectrum och publiceras i denna uppsats med ett godkännande av upphovsmannen)*

## 5.2 Hotbilder

Tack vare den välutvecklade teknologin och de välkonstruerade datorer som alla människor mer eller mindre har tillgång till, har cyberhoten blivit allt fler. Man kan säga att: Ju fler – desto mindre kontroll.

Idag kan vem som helst utföra en attack, det kan vara en ungdom som har tråkigt hemma. Där denne kanske vill testa sina färdigheter eller göra något som är utöver det vanliga och mer spännande. Därmed kan denne försöka hacka sig in i ett system, för att överbelasta det. Det kan även vara grupper som obemärkt och strategiskt försöker slå ut sin fiende. Det är dock vanligt att dessa attacker och aktörer är ute efter en sak, att orsaka en skada eller att försöka tjäna pengar.

Sabotage är den ”vanligaste” formen av attack, som utförs idag[3]. Men sabotage kan även omfatta stora överbelastningar och ned stängning av nätverkssystem, för att visa sitt missnöje. Precis som *Anonymous* gjorde mot den svenska staten. *Ett utdrag från Göteborgsposten om attacken, [22]:*

Vid halv tre slutade flera officiella sajter att fungera. Sweden.se, riksbank.se, domstol.se, Antipiratbyrån och Säkerhetspolisens tre hemsidor låg nere. På Kriminalvårdens sida stod ett officiellt meddelande där det stod att sidan hade begränsad funktionalitet.

Troligen beror detta på Anonymous attacker. Flera av de nämnda adresserna har lagts upp som bilder på den facebookside som tillhör gruppen Anonymous squad 035, under hashtaggen #TANGODOWN.

– Jag kan bekräfta att vår sida ligger nere och att våra tekniker arbetar med att lösa det, säger Sara Kvarnström, som är pressekreterare på Säpo till GP, vid 16-tiden.

– Jag vill inte spekulera i vad det här beror på men vi har sett ökad aktivitet på vår hemsida på eftermiddagen. Vi har vidtagit en del åtgärder som kan göra det svårt för besökare att ta sig in på vår sida, säger Sara Kvarnström. [22].

Enligt en publikation av *National Institute of Standards and Technology*, “*Guide to Industrial Control Systems (ICS) Security*”, skiljer sig syften med attackerna - beroende på vem som utför attacken [27]. Ett exempel som tidigare har nämnts, är att terrorister nästan alltid är ute efter att försvaga sin fiendes ekonomi, döda människor, eller utnyttja infrastrukturen. För att utgöra hot mot den nationella säkerheten.

Det som skulle kunna vara i deras intresse, är informationssamling. Just för att på ett strategiskt sätt kunna utföra en dödlig markattack.

Information är värdefull idag och människor gör vad som helst för att komma åt den. När det är svårare att komma åt viss information finner människor mer intresse i det, att anta utmaningen samt se nöjet i att kunna ”knäcka” något som kan vara svåråtkomligt [78]. Människor gör ofta detta just för utmaningens skull. De kan under press och ”rätta omständigheter” jobba för grupper som ägnar sig åt olagliga aktiviteter. Informationen kan säljas vidare utan att man tänker på konsekvenserna.

Ett annat exempel är en artikel som nyligen publicerades av *The New York Times*, "Cyberattack seem to meant to destroy, Not just disrupt", [5]. Artikeln handlar om att numera attacker ska förstöra än spionera. Det man tidigare hade fruktat har blivit en verklighet – en svaghet.

Attacker mot de ekonomiska institutioner är ett bevis på att jakten på kraftfullare cyber-attacker har blivit lika hett som jakten på kärnvapen. De senaste attacker mot *American Express*, har kostat företaget miljontals dollar och försatt dem i en position där man lägger ner massvis med resurser för att öka säkerheten. Just för att sådana attacker inte ska kunna inträffa igen.

Länder som Iran och Nordkorea, är inte längre inställda på att stjäla information. De är istället ute efter att med hjälp av cyber-attacker skada ett land.

I jakten på kraftfullare cyber-attacker, ökar möjligheten till att dessa sprids till en helt annan plattform, smarta mobiler. Mobiler är något som alla bär med sig dagligen och de har blivit en stor del av våra liv, något som i stort sätt varje människa äger. Vi är nästintill beroende av dessa telefoner och de spelar en stor roll i vårt vardagliga liv. Då vi skickar sms, ringer, använder oss av kalendern, använder olika applikationer som vi har laddat ner till våra telefoner, skickar bilder, skickar videospelningar, använder videosamtal, söker efter diverse genom internet osv. En teknik som har blivit en vana för oss och vanan har blivit en bekvämlighet, och just därför är det svårt att klara sig utan dessa telefoner.

Innan använde man endast mobiler för att ringa, vilket också var syftet. Då de skapades just för det från allra första början. Tekniken har gått så långt fram, att mobiltelefonerna är mycket mer utvecklade än så, mycket mer avancerade.

Idag använder vi bankdosor som ger oss tillgång till våra banker med hjälp av internet, där vi betalar räkningar, beställer hem prylar som vi betalar med hjälp av bankdosan. Idag ä det inte många som går och bär på kontanter, just på grund av att det finns möjligheter där man kan använda sig av bankkortet istället. Den elektroniska användningen av bankkort utgör en stor del av vår fungerande vardag.

Idag får man till och med mail där man uppmanas att knappa in sitt kontonummer och eventuellt ytterligare koder. I mailet uppmärksammar man användaren på att kontot har blivit utsatt för intrång och att kontot måste återställas. Enligt mailet så gör man detta genom att knappa in sin kod och således kan en tredje part göra ett intrång och rensa kontot.

En annan publikation som publicerades av *James Andrew Lewis*, "Significant Cyber Events", *Center For Strategic & International Studies*, visar rapporterade cyberattacker från 2006- februari 2013 [9]. Nedan följer några av attackerna:

- **September 2011.** A computer virus from an unknown source introduced "key logger" malware onto ground control stations for US Air Force UAVs and, according to press reports, infected both classified and unclassified networks at Creech Air Force Base in Nevada. The US did not lose control of any drone nor does it appear that any data was exfiltrated, but the malware was persistent and took several attempts to remove [9].
- **October 2011.** Networks of 48 companies in the chemical, defense and other industries were penetrated for at least six months by a hacker looking for intellectual property. Symantec attributes some of the attacks to computers in Hebei, China [9].
- **November 2011.** Apple computers belonging to European Commission officials, including EC Vice President for the "Digital Agenda," were hacked at an Internet Governance Forum (IGF) meeting in Azerbaijan [9].
- **March 2012.** NASA's Inspector General reported that 13 APT attacks successfully compromised NASA computers in 2011. In one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems. Another attack at the Joint Propulsion Laboratory involving China-based IP let the intruders gain full access to key JPL systems and sensitive user accounts [9].
- **April 2012.** Iran was forced to disconnect key oil facilities after a cyber-attack against internal computer systems. The malware was found inside the control systems of Kharg Island – Iran's main oil exporting terminal. Equipment at Kharg Island and at other Iranian oil plants has been disconnected from the internet as a precaution. Iran reported that oil production was not affected, but the websites of the Iranian oil ministry and national oil company were forced offline and data about users of the sites was taken as a result of the attack [9].
- **April 2012.** A hack of Japan's Ministry of Agriculture, Forestry and Fisheries resulted in more than 3,000 documents exfiltrated to a foreign destination, including 20 classified documents on negotiations on the Trans-Pacific Partnership (a broad free-trade agreement). According to press reports, the hackers searched Ministry computers for TPP documents, transferred all that were found to a single computer, and then compressed them to make them easier to send [9].
- **September 2012.** Izz ad-Din al-Qassam, a hacker group linked to Iran, launched "Operation Ababil" targeting bank websites for sustained denial-of-service attacks. Targets include Bank of America, New York Stock Exchange, Chase Bank, Capital One, SunTrust, and Regions Bank [9].
- **October 2012.** The Russian firm Kaspersky discovered a worldwide cyber-

*attack dubbed “Red October,” that had been operating since at least 2007. Hackers gathered information through vulnerabilities in Microsoft’s Word and Excel programs. The primary targets of the attack appear to be countries in Eastern Europe, the former USSR and Central Asia, although Western Europe and North America reported victims as well. The virus collected information from government embassies, research firms, military installations, energy providers, nuclear and other critical infrastructures, although the full extent of the damage is unknown [9].*

- **January 2013.** *Izz ad-Din al-Qassam claims responsibility for another series of distributed denial-of-service attacks against US Bank websites, as part of “Operation Ababil,” phase two. Targets include: Ally Financial, BB&T, Capital One, Fifth Third Bank, HSBC, PNC, Wells Fargo, SunTrust, and Zions Bank. US officials speculate that the group is a front for a state-sponsored campaign attributed to Iran [9].*
- **February 2013.** *The Department of Homeland Security issued a restricted report, revealing that from December 2011 through June 2012, cyber criminals targeted 23 gas pipeline companies and stole information that could be used for sabotage purposes. The report does not mention China, but experts trace the digital signatures of the attacks to a Chinese cyber espionage group [9].*

## 6. Artiklar

I detta stycke kommer jag att presentera en sammanställning av de olika artiklarna. Artiklarna används som grund för denna uppsats, sammanfattningen kommer att ske utifrån mina valda nyckelord.

### 6. 1 Artikel A)

*"Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats", James A. Lewis, Center for Strategic and International Studies, December 2002, [1].*

Artikeln relaterar främst till cyber-terrorism och cyber-attacker mot infrastrukturen och hoten mot den nationella säkerheten i USA.

En stor omfattning av litteraturen som är relaterad till dessa ämnen anser att sårbarheten mot dessa system är extremt stora menar *James A. Lewis*. Litteraturen menar att den nationella säkerheten är i fara, ifall en grupp av onda människor skulle bestämma sig för att utföra en robust cyber-attack.

Författaren har en helt annan uppfattning, han menar att dessa system samt nätverk är så komplexa att man inte skulle kunna skada dem på något sätt. Med tanke på detta, anser författaren att cyber-attacker är obetydliga, jämfört med fysiska attacker.

Även hoten mot den nationella säkerheten kan anses som överskattade. På en nationell nivå är systemen så komplexa, att det uppgår uppemot etthundra olika system, som är ihopkopplade på något sätt, för att allting ska fungera på rätt sätt.

För att cyber-terrorister överhuvudtaget ska utgöra det minsta lilla hot mot den nationella säkerheten, hade man varit tvungen att attackera flera system samtidigt under långa perioder. Även då hade man inte kunnat skapa någon oro på nationell nivå.

Artikeln tar upp några exempel där man jämför cyber-attacker med fysiska attacker. Inte ens vid fysiska attacker är man kapabel till att slå ut ett lands infrastruktur, av en enda attack.

När andra världskriget pågick, utsattes Tyskland för fysiska attacker. Men först vid ständiga flygattacker lyckades man slå ut och paralysera infrastrukturen.

Författaren menar att det enda sätt som finns för att kunna lyckas med en cyber-attack, är ifall man fortsätter att utveckla system. Utan att öka deras säkerhet, vilket troligtvis aldrig kommer att ske.

Fastän dessa cyber-attacker oftast anses vara riktade mot militären, är det inte troligt att ett land försätter sin militära styrka i ett sådant läge. Där de helt och hållet är beroende av datanätverk.

Ett uppmålat scenario är att en hackare, terrorist eller utländska spioner, skulle med några rader av kod kunna utgöra hot mot den nationella säkerheten och därmed slå ut komplexa samhällssystem. System allmänheten är beroende av. Detta scenario är något som är utan bevis. Terroristen skulle möjligtvis kunna använda sig av internet, för att komma åt hemlig information. Eller stulna kreditkort, för att finansiera sina fysiska attacker. En sofistikerad attack skulle kunna vara att man obemärkt hackar sig in i ett system, endast för att samla information. Författaren menar att rutinmässiga fel, kraschande system, skadar och kostar mer än en cyber-attack.

*“Once a hacker has gained access and the damage done, the target usually responds quickly to close off the vulnerability that allowed that line of attack and to bring systems back on line. Cyber attackers would continually need to exploit new vulnerabilities and new tactics to ensure sustained disruption. Cyber-attacks also seldom if ever produce physical damage that requires time-consuming repairs.”[1].*

## 6. 2 Artikel B)

*”Cyber war will not take place”, Thomas Rid, 05- October 2011, [3].*

Denna artikel handlar om att författaren Thomas Rid argumenterar emot och tycker att ett cyber-war aldrig kommer att inträffa. Enligt honom så måste en attack uppfylla vissa kriterier för att det skall räknas som en krigshandling. Kriterierna är att attacken måste leda till dödsfall och attacken måste ha en politisk inblandning.

Thomas Rid försöker förklara ordet cyber-war och innebörden med cyber-attacker med hjälp av många olika exempel. Exempel som handlar om möjliga scenarion som kan uppstå och möjliga skador som dessa attacker kan föra med sig. En av attackerna som betraktas som historiens värsta är explosionen av en rörledning i Sibirien år 1982. Strax efter attacken hemligstämplade FBI alla dokument och bevis som hade med explosionen att göra, därför kommer man aldrig få reda på ifall det verkligen orsakades av en cyber-attack.

Ett annat exempel som Thomas Rid tar upp är intrånget i NASA. Attacken och stölden av dokumentation pågick i nästan två år innan man upptäckte det. I det här fallet fanns det varken några konkreta syften med attacken, våld eller politisk inblandning.

Ingen attack i historien uppfyller dessa kriterier. Sabotage, spionage och upproriska aktiviteter har använts i århundraden menar Thomas och dessa kommer naturligtvis fortsätta att bistå i militära operationer.

*“Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future. Instead, all past and present political cyber-attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage.” [3].*

*“The question is if a trend is leading to inevitable acts of stand-alone cyber war, with code as the main weapon, not as an auxiliary tool that is nice to have.” [3].*

### 6.3 Artikel C)

*"Cyberwar Thresholds and Effects", James A. Lewis, Center for strategic and International Studies, September/October 2011, [2].*

Artikeln visar hur cyber-war egentligen ser ut och granskar hur man kan dra nytta av en cyber-attack. Författaren skriver att cyber-attacker inom det militära väsendet är oundvikliga, och att de inte bör skilja sig så mycket från dem fysiska attacker. Om en attack inte innehåller något slags hot eller någon slags våld så räknas det inte som en attack. Skulle en aktör obemärkt hacka sig in i ett system utan att utgöra någon fysisk skada, kan det varken räknas som våld, -attack eller hot. Cyber-attacker tillåter aktören från distans att kunna utföra skador på nätverksbaserade tjänster och mot infrastrukturen. Det kan bidra till taktiska och strategiska fördelar men han menar att en attack sällan kan frambringa seger på egen hand.

Enligt publikationen så kan attacker sträcka sig längre än så och verkligen orsaka fysiska skador vilket bevisades i Idaho National Labs, där man med hjälp av en sådan attack pressade en elektrisk generator till självförstörelse. Trots all detta så kan man inte utföra en cyber-attack med precision. Möjligheten föreligger till att attacken sprider sig till oönskade ställen som i sin tur kan orsaka politiska problem.

En cyber-attack är en engångsattack som innebär att varje gång man utför en attack så är man tvungen till att konstruera nya medel för att ytterligare kunna utföra attacker. Samtidigt som man konstruerar medel för en ny attack så ökar säkerheten hos den som har blivit utsatt. Det har varit få incidenter där länder har utfört sådana cyber-attacker mot varandra.

Författaren skriver att länder som Iran och Nordkorea är mer benägna till att utföra skadliga cyber-attacker mot USA jämfört med mindre och svagare länder. Skulle ett litet land utföra en liknande attack mot USA där man skadar landet på en nationell nivå så hade det lett till en invasion.

Fastän nästan allting är tillåtet i krig, så måste man beakta vissa regler när man skall utföra en cyber-attack. Att utföra attacker mot civila mål såsom infrastrukturen kräver en viss bedömning. En militär fördel måste ligga till grunden för att kunna utföra en cyber-attack. Troligtvis så görs inte dessa bedömningar av rebeller och terrorister.

*"We know from experience that a networked force is more effective than a non-networked force of similar size. Networked air defense is appreciably more effective than an aggregation of individual units. Nation-states with armored vehicles, aircraft, and ships connected by data links will fight more effectively than their counterparts who rely solely on voice. This increase in effectiveness makes military networks legitimate and valuable targets. Network technology use and cyberspace exploitation for intelligence and attack have become a normal part of military activity." [2].*

## 6.4 Artikel D)

*"Panetta Warns of Dire Threat of Cyber-attack on U.S.", Elisabeth Bumiller and Thom Shanker, The New York Times, October 11-2012, [6].*

Denna artikel handlar om ett uttalande av försvarsministern, Leon Edward Panetta. Detta uttalande gjordes vid Intrepid Sea, Air and Space Museum i New York.

Panetta menar att USA befinner sig i ett underläge gentemot sina motståndare som är Kina, Ryssland, Iran och militanta grupper. Panetta reagerade på deras ökade aggressivitet och tekniska framsteg. Enligt Panetta befinner sig USA i ett sårbart tillstånd där möjligheten för en "cyber-Pearl Harbor" föreligger. Ett tillstånd som är så pass sårbart att utländska hackare kan avveckla kraftnätet, transportsystemet, ekonomiska nätverk samt regeringen.

Ett exempel som Panetta uppgav är:

*"An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches," Mr. Panetta said. "They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country." [6].*

Panettas uttalande om en möjlig "cyber-Pearl Harbor" förklarades som ett scenario där flera cyber-attacker mot infrastrukturen utförs på en och samma gång. Tillsammans med en fysisk attack skulle detta innebära en fysisk förödelse och förlust av många liv. En sådan attack hade paralyserat och chockat nationen och därmed skapat en ny mening av begreppet sårbarhet.

Försvarstjänstemän menade att Panettas uttalande inte var överdrivet, utan att det var en reaktion på den senaste vågen av cyber-attacker som gjordes mot de ekonomiska institutionerna. Panettas uttalande var också en reaktion på en attack som utfördes i augusti mot det statliga oljebolaget Saudi ARAMCO där en cyber-attack utfördes och orsakade att mer än 30,000 datorer blev oanvändbara.

*"The United States won't succeed in preventing a cyber-attack through improved defenses alone." [6]*

*"If we detect an imminent threat of attack that will cause significant physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us, to defend this nation when directed by the president," Mr. Panetta said. "For these kinds of scenarios, the department has developed the capability to conduct effective operations to counter threats to our national interests in cyberspace." [6].*

## 6.5 Artikel E)

*"Obama Order sped up wave of Cyber-attacks against Iran", David E Sanger, The New York Times, June 1-2012, [7].*

Denna artikel handlar om hur USA för första gången lyckades att paralysera en infrastruktur i ett annat land, med hjälp av en datorkod. Denna Cyber-attack blev kallad för "Olympic Games". Den blev allmänt känt på grund av ett programmeringsfel under sommaren 2010.

Detta var ett virus som skulle slå ut kärnkraftverk i staden Nantanz, som ligger i Iran. Attacken misslyckades och Obama fattade ett viktigt beslut då han beslöt att utvecklingen av viruset skulle fortsätta, för att återigen försöka förstöra kärnkraftverket. Flera cyber-attacker utfördes och man lyckades slå ut 1000 av de 5000 centrifugerna som framställer uran. Cyber-attacken fick namnet "Stuxnet".

En medhjälpare till Obama gjorde ett uttalande, där han sa att: *"If Olympic Games failed, he told aides, there would be no time for sanctions and diplomacy with Iran to work. Israel could carry out a conventional military attack, prompting a conflict that could spread throughout the region."*

Obama sa däremot: *"When it came to stopping Iran, the United States had no other choice."*

Iran förnekade denna attack och dess påverkan på centrifugerna, och de menade istället att man oskadliggjorde viruset. Generalen Gholamreza Jalali har dock meddelat att Iran har tillsatt en egen cyberenhet som är beredda: "To fight our enemies" in "cyberspace and Internet warfare.". Det finns inte tillräckligt med bevis som styrker hans uttalande.

Trots att USA har medgett att landet utvecklar cyber-vapen, har man aldrig riktigt erkänt att man har använt dem i något sammanhang. Anledningen till detta är att oron av att andra länder, terrorister och hackare kan rättfärdiga sina egna attacker.

*"We've considered a lot more attacks than we have gone ahead with", sa en före detta underrättelseofficer. [7].*

Obama har upprepade gånger talat om för sina medhjälpare om risken med att använda sig av denna typ av vapen. USA är ett land som är så beroende av datorsystem att detta försätter dem i en sådan position att dem är mer sårbara än något annat land i världen. Många experter tror att det bara är en tidsfråga innan länder börjar använda sig av samma slags vapen som USA använde sig av mot Iran.

## 6. 6 Artikel F)

*“Cyber-attacks seem Meant to Destroy, Not Just Disrupt”, Nicole Perlroth and David E. Sanger, The New York Times, March 28-2013, [5].*

Artikeln tar upp några exempel på välutförda och lyckade cyber-attacker mot bland annat USA och Sydkorea. Författaren skriver att länder så som Iran och Nordkorea inte längre är ute efter att spionera samt stjäla information, de är ute efter att förstöra. Med hjälp av dagens teknologi kan man orsaka stora ekonomiska förödelse mot länder, med hjälp av en skadlig kod.

Ekonomiska institutioner har blivit nya mål för denna slags attacker. Nyligen orsakade dessa attacker skador för miljontals dollar. Institutioner som blev utsatta för detta är bland annat American Express, JP Morgan Chase, Bank of America, bara för att nämna en del.

Obama-administrationen har uppmanat till att utsatta företag bör tillkännage utförda cyber-attacker. Men på grund av en upptäckt sårbarhet, ger säkerhetsexperter och advokater motsatta råd.

För länder som Iran och Nordkorea så är dragningskraften för cyber-vapen lika stor som mot kärnvapen.

*“These countries are pursuing cyber weapons the same way they are pursuing nuclear weapons,” said James A. Lewis, a computer security expert at the Center for Strategic and International Studies in Washington. “It’s primitive; it’s not top of the line, but its good enough and they are committed to getting it.” [5].*

*“We don’t know how they make decisions. When you add erratic decision making, then you really have something to worry about.” [5].*

## 6. 7 Artikel G)

*“ATM thieves conducted massive cyber-attack”, Zachary A. Goldfarb, The Washington Post, May 09-2013, [8].*

Denna artikel handlar om hur organiserad brottslighet har lämnat ifrån sig sina pistoler och bytt ut dem mot datorer. Attacken som utfördes mot dem finansiella företagen i USA och Indien var den första i sitt slag. Aktörerna lyckades hacka sig in i deras system och således ta bort uttagsgränsen för kreditkort.

Det var enbart banker och inte enskilda personer som blev drabbade av denna attack. Ligan som tog ut pengarna i kontanter lyckades få med sig 45 miljoner dollar. Det man nu fruktar är att i takt med den teknologiska utvecklingen kan dessa attacker bli fler och mer förödande.

*“The first thing the card business is trying to do is to make it easier for people to transact,” Brian Riley senior director at CEB Tower Group said. “As you do that, you’re opening up new areas to get attacked in. You’re opening up new vulnerabilities that never existed.” [8].*

## 6.8 Artikel H)

*“Cyber war will take place!”*, John Stone, 2013, [4].

Författaren till denna artikel demonstrerar att ett cyber-war kan bryta ut trots åtskilliga motargument. Anledningen till att pågående debatt kring ämnet inte kan komma till en konkret slutsats, är för att man inte riktigt kan precisera vad krig i sig utgör.

För att styrka sin ställning använder sig författaren av en studie som är publicerad av Thomas Rid, ”cyber war will not take place”, se avsnitt 6.2, artikel B, som menar att en cyber-attack kan vara ett tillägg till en krigshandling. Men som inte utgör en sådan handling i sig. Nedan följer ett avsnitt som Thomas Rid använder sig av för att stärka sin ställning kring ämnet.

*“War is an act of force to compel our enemy to do our will”, wrote Carl von Clausewitz on the first page of On War. All war, pretty simply, is violent. If an act is not potentially violent, it is not an act of war . . . A real act of war is always potentially or actually lethal, at least for some participants on at least one side.”*[4].

Författaren skriver att all slags krig omfattar någon slags kraft. Men inte nödvändigtvis våld särskilt om våld innebär dödsfall. För att stärka sitt uttalande använder sig författaren av Clausewits förklaring, ”War, as an act of force”.

Ett exempel som författaren tar upp:

*“One example is a stabbing to death with a stiletto gently slid between the ribs . . . a second example (or class of examples) concerns poisoning or gassing.”* [4].

Med denna jämförelse menar författaren att man med hjälp av teknologin kan skapa mängder av kraft som kan orsaka stor förödelse. Jämförelsen poängterar att en cyber-attack utgör ett effektivt sätt att överföra kraft till våld. Några rader av kod kan försätta ett tåg i en händelse med våldsamma konsekvenser.

Som slutsats av artikeln och för att stärka sina argument så skriver författaren följande:

*“In conclusion, cyber war is possible in the sense that cyber-attacks could constitute acts of war. This point only becomes evident, however, if we are clear about what is encompassed by the terms ‘force’ and ‘violence’, and about their relationship with the matter of lethality. Acts of war involve the application of force in order to produce violent effects. These violent effects need not be lethal in character: they can break things, rather than kill people, and still fall under the rubric of war. Moreover, the mediating influence of technology means that small acts of force – such as tapping a keyboard – can result in large amounts of violence, lethal or otherwise.”* [4].

## 7. Jämförelse av material

I följande kapitel, kommer jag att redogöra en jämförelse av det valda materialet. För att klargöra vad författarna säger om cyber-war, om det bara är ett förstorat ämne eller om det är något som vi ska ta på allvar?!

I artikel A och artikel C har vi samma författare men publikationerna är utgivna år 2002 respektive år 2011. Artikel B är en författare som sågar teorierna om cyber-war, argumenterar emot och lägger fram fakta för att stärka sin ställning i ämnet där han menar att cyber-war inte kommer att ske.

Artikel C definierar ordet cyber-war som en teknik som används för att orsaka skada, förödelse och något som leder till försluter för politisk effekt, för stater eller politiska grupper. För att svara på definitionen om cyber-war i artikel C, säger artikel B att det inte finns någon cyber-attack som uppfyller kriterierna för att det ska framstå som en krigshandling. Kriterierna är att en attack måste vara våldsam, förstärkande och politisk, för att det ska räknas som cyber-war.

Definition av ordet cyber-war i artikel C styrks även av författaren i artikel H, som menar att en cyber-attack används på ett effektivt sätt, för att kunna överföra kraft till våld. Några rader av en viss kod kan orsaka stora förödelse, skriver författaren i artikel H.

Ett av kriterierna som en cyberattack måste omfatta. Är att den måste vara våldsam, enligt författaren i artikel B. Vilket leder oss återigen till artikel H, där författaren skriver att en attack är en teknik där man kan överföra kraft till våld.

Thomas Rid skriver i artikel B att en attack aldrig har orsakat en förlust av ett människoliv. Artikel A har nästan samma åsikt som artikel B genom att den skriver att en cyber-attack är mindre skadligt, än en fysisk attack. De har aldrig skadat en byggnad eller överhuvudtaget skadat en person, vilket stärker argumentet som står i artikel B.

Påstående hittar motargument både i artikel D respektive artikel H. Författaren i artikel H ger ett exempel, som motsvarar samma svar som i artikel D, där man tar ställning gentemot argumentet som står i artikel B. Fortsättningsvis kan vi styrka ställningen i artikel H, att en cyber-attack är en teknik som kan överföra kraft till våld, genom artikel E. Där USAs försvarsminister Leon Edward Panetta sa följande:

*“An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches,” Mr. Panetta said. “They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country.” [6].*

Det hade kunnat resultera i storskaliga dödsfall.

Ett annat kriterium som artikel B tar upp, är att en attack måste vara politisk. Artikel E är ett utmärkt motargument till artikel B. Författaren i artikel E skriver att USA lyckades paralysera en infrastruktur i ett annat land med hjälp av datakod.

Enligt forskningen i artikel A skriver författaren att nationer är mer stabila, än vad analytiker tidigare har trott. Artikeln säger att infrastrukturens system rutinmässigt utsätts för brott. Att attacker därför är mer flexibla och robusta till att återställa servicen, än vad analytiker tidigare har trott.

Detta påstående motbevisas i artikel D. Där man menar att USA är i ett så pass sårbart tillstånd att utländska hackare med hjälp av en cyber-attack kan avveckla kraftnätet, transportsystemet, ekonomiska nätverk och regeringen. Allt detta styrks av artikel E, där USA lyckades paralysera infrastrukturen. Genom att förstöra centrifuger som framställer uran i Iran.

Artikel C skriver: ”Cyber-war kommer att innebära avbrott i viktiga data och nätverkstjänster samt skador på infrastrukturen. Det kommer även att skapa oro och tvivel bland dem motstående politiska ledare och befälhavare.”

Samma författare skriver i artikel A att moderna industriella samhällen, är mer robusta än man tror. Han skriver även att infrastrukturen i ekonomiskt starka länder är mer uppdelade, olika, överflödiga och mer självläkande än vad man tror. Medan artikel D och E skriver att USA är i ett sårbart tillstånd och detta bekräftas av en våg av olika attacker som utfördes mot ekonomiska institutioner som tas upp i artikel F.

För att ytterligare styrka uttalandet i artikel D, om sårbarheten. Används det ett exempel, där en cyber-attack mot det statliga oljebolaget Saudi ARAMCO orsakade att mer än 30,000 datorer blev oanvändbara. Artikel F och G tar upp utförda attacker mot ekonomiska institutioner, som orsakade skador för miljontals dollar. Även dessa artiklar är starka motbevis för påståendet i artikel A.

Att försöka skada infrastrukturen, är något som artikel C tar upp. Författaren skriver att en möjlig attack mot sjukhusystemet, kan medföra dödsfall. Ett exempel som motargument för detta påstående, tas upp i artikel A. Författaren menar, om en cyber-attack utförs mot ett sjukhus, hade man kunnat ändra journaler hos patienterna vilket hade lett till en stor förvirring innan man hade kunnat vidta några åtgärder. Patienter hade kanske fått fel behandling eller fel medicin vilket hade kunnat leda till dödsfall om patienten är väldigt sjuk. Under kriterierna som författaren i artikel B tar upp, att kraven för en krigshandling i denna attack, inte uppfylls. Just en sådan attack skulle kunna vara av intresse för terroristgrupper.

Artikel A skriver om att terroristernas handlingar oftast är våldsamma, och att de är ute efter att göra så stor skada som möjligt. Artikeln förklarar detta genom att terrorister vill att handlingarna som utförs i deras namn ska synas och höras. En cyber-attack skulle vara obemärkt för allmänheten och det är inte något som terrorister är ute efter.

Att cyber-attacker inte är av intresse för terrorister, för oss vidare till artikel B som säger att spionage är den sofistikerade versionen av så kallad "cyber-attack", något som terrorister hade kunnat dra nytta av. I artikel F skriver författaren att länder så som Iran och Nordkorea inte längre är ute efter att spionera och stjäla information, utan att förstöra.

Ett exempel som skrevs i artikel C, är den elektriska generatoren som självförstördes med hjälp av en "cyber-attack". Artikel A skriver däremot att erfarenheten inom ämnet, har visat att cyber-attacker måste vara kontinuerliga och många för att utgöra någon skada. Man hade varit tvungen att ständigt komma med nya medel och taktik, för att utföra en sådan skada. Både artikel A och C skriver att en cyber-attack är något som kan utföras endast en gång.

Påståenden i meningarna ovan som artikel C och artikel A tar upp, är något som styrks av artikel E. Författaren i artikel E, skriver om en misslyckad attack. Efter den misslyckade attacken fortsatte man med att utveckla viruset. För att återigen utföra en cyber-attack, denna gång en lyckad attack.

Blir man utsatt för en attack eller ett intrång, ökar man säkerheten för att något liknande inte ska kunna inträffa igen. Enligt Panetta i artikel D, kommer USA inte att kunna förhindra en cyber-attack enbart genom att förbättra säkerheten.

Artikel A skriver att dessa attacker är mer lika sabotage, än cyber-war. Fastän författaren i artikel C tidigare gav ett exempel på en skadlig attack, skriver författaren "enbart cyber-attacker kan inte medföra någon seger". Vilket stärker teorierna som står i både artikel A och i artikel B gällande cyber-krigföring. Detta för oss vidare till artikel D, där Panetta talade om en möjlig "cyber-Pearl Harbor". Panetta förklarade detta som ett scenario, där flera antal cyber-attacker på en och samma gång utförs mot infrastrukturen. Tillsammans med en fysisk attack skulle detta innebära fysisk förödelse och förlust av många liv. En sådan attack hade paralyserat och chockat nationen och därmed skapat en ny mening av sårbarhet.

Artikel C menar att länder inte vågar utföra skadliga attacker, på grund av att dessa inte kan utföras med precision. Skulle ett land ändå bestämma sig för att utföra en sådan attack, finns risken till att attacken sprider sig till länder som inte är involverade i konflikten. Det i sin tur skulle medföra politiska påföljder. Med tanke på detta, stärks även här teorierna om krigshandling av författaren B, som menar att ett av kriterierna för krigshandling är en politisk inblandning.

Obama-administrationen har uppmanat till att utsatta företag bör tillkännage utförda cyber-attacker. Men på grund av en upptäckt av sårbarhet ger säkerhetsexperter och advokater motsatta råd, skriver författaren i artikel F. Författaren i artikel E, skriver att många experter tror att det bara är en tidsfråga. Innan länder börjar använda sig av samma slags vapen, som USA använde sig av mot Iran. Men samtidigt står det, trots att USA har medgett att landet utvecklar cyber-vapen, har man aldrig riktigt erkänt att man har använt dem i något

sammanhang. Anledningen till detta är oron av att andra länder, terrorister och hackare kan rättfärdiga sina egna attacker.

I artikel A beskrivs det om ett scenario där en terrorist, hackare eller utländska spioner med några rader av kod kan ta över en hel nation eller skada infrastrukturen, är något som är utan bevis. Det kan naturligtvis bero på att regeringar inte riktigt presenterar vilka lyckade attacker man har blivit utsatt för och hur skadliga dessa har varit, skriver författaren i Artikel B.

Påståendet leder oss till artikel E, där en sådan attack lyckades och samtidigt förnekades.

Från ett militärt perspektiv, är det inte av stor betydelse och heller inte ett hot mot den nationella säkerheten om en attack inte orsakar mer skada än de rutinmässiga felen, skriver författaren i artikel A. Om en attack inte följs upp av en fysisk attack så är effekten inte alls stor enligt artikel A. Av exemplet som tidigare nämnts i artikel C skriver författaren att en cyber-attack kan ses som ett långdistansangrepp eftersom de är snabbare än missiler, men mycket billigare att tillverka.

Detta för oss återigen till ett Panettas uttalanden:

*“If we detect an imminent threat of attack that will cause significant physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us, to defend this nation when directed by the president,” Mr. Panetta said. “For these kinds of scenarios, the department has developed the capability to conduct effective operations to counter threats to our national interests in cyberspace.” [6].*

Och vidare till artikel F och artikel G, där skadorna uppskattades uppemot miljontals dollar.

Artikel C och A delar samma åsikt om att det är billigare att utföra en cyber-attack än en fysisk attack. Författaren i artikel A skriver att det enda som kan behövas är en tonåring och en dator. Författaren i artikel C skriver, trots att utrustningen är billigare, så är det mycket dyrare att planera och utföra en attack. Det man måste ha i åtanke är allt förarbete som krävs för att planera en attack, som t.ex. att försöka hitta sårbarheten i nätverkssystemet. Man måste ständigt jobba vidare med utvecklingen, lägga till eller ändra mjukvaran följaktligen till systemet som man ska utsättas för en attack.

Författaren i artikel B skriver:

*“Digital networks are a new tool for state power, and cyber-attack will be part of future military conflict. Like earlier technological innovations, it will reshape warfare. Unfortunately, some of the issues and ambiguities identified in this article won’t be resolved until we gain more direct cyber warfare experience.”[3].*

Som för oss vidare till vad författaren i artikel C skrev:

*“Cyber war has never happened in the past, that cyber war does not take place in the present, and that it is unlikely that cyber war will occur in the future.”[2].*

## 8. Diskussion

Utifrån valda publikationer, har jag lyckats med att få en bättre förståelse inom ämnet cyberwar. Precis som David E. Sanger skriver i artikel E, att USA är beroende av datorsystem, så är människornas liv också beroende av det. Majoriteten av de saker vi gör kretsar kring datorstyrda enheter och system. Ju mer beroende vi blir av teknologin desto sårbarare blir vi. Genom artiklarna som har presenterats i min studie, kan man se tydliga tecken på att det kommer utföras allt mer aggressiva och skadligare attacker framöver [89, 90].

Finansiella institutioner som länge ansetts som säkra system [91, 92, 93], har nu blivit ett utsatt mål för cyberattacker [8]. Efter att ha läst om ämnet i en rad av olika publikationer, drog jag slutsatsen om att länder inte riktigt vågar erkänna sina utförda cyberattacker. Detta bekräftas bland annat av David E Sanger som i analys E skriver, att USA aldrig har erkänt sina attacker. Om USA inte vågar erkänna sina utförda cyberattacker, kan detta möjligtvis betyda att rädslan för dessa attacker kan vara stor?

I takt med teknologins framfart, kommer även attackerna att utvecklas och förfinas allt mer och mer. Attackmålen kommer även därmed att i högre grad bli fler och potentiellt sett skulle kunna utsätta allt fler och fler människor för påtaglig fara [94, 95, 96, 97].

Med digitaliseringen utsätter vi oss själva i fara för möjliga attacker. Attacker som i framtiden kommer att kunna angripa individuella hem, då våra liv kretsar kring enheter samt system, som vi ständigt har runt om oss. Än idag har vi inte lyckats hitta en tillräckligt bra lösning för att kunna skydda oss mot olika slags cyberattacker [98, 99, 100].

Med all fakta som presenterats i denna uppsats, vill man gärna tro att det finns en lösning och ett skydd mot cyber-attacker. Med detta sagt, är allt skapat av människan och då måste människan väl också kunna stoppa det? Men det kanske är något som inte helt och hållet kan gälla i detta sammanhang? Det kanske skulle innebära att Internet måste börja om från noll igen för att man på något sätt ska återfå kontrollen. Vilket i dagsläget är omöjligt eftersom vi är så pass beroende av dagens teknik samt kommunikationssättet som vi har skapat [65, 66]. Därför måste man kanske definiera begreppet lika tydligt som författaren i artikel H gör och skriver:

*“In conclusion, cyber war is possible in the sense that cyber-attacks could constitute acts of war. This point only becomes evident, however, if we are clear about what is encompassed by the terms ‘force’ and ‘violence’, and about their relationship with the matter of lethality. Acts of war involve the application of force in order to produce violent effects. These violent effects need not be lethal in character: they can break things, rather than kill people, and still fall under the rubric of war. Moreover, the mediating influence of technology means that small*

*acts of force – such as tapping a keyboard – can result in large amounts of violence, lethal or otherwise.” [4].*

## 9. Slutsats

Det finns dem som hävdar att cyberkrig helt enkelt är ett förstorat ämne. Motsatt finns det även dem som faktiskt är övertygande om att cyberattacker utgör ett reallt hot. Dessa två olika synvinklarna är själva kärnan i uppsatsen. Utifrån analysen är det svårt att svara på forskningsfrågan om det är någon som har rätt eller fel, trots att majoriteten i min studie (*Tabell 1*) anser att det är ett hot.

För att kunna besvara forskningsfrågan måste man förbestämma vad ordet hot innebär. Ett hot kan vara allt från att man stänger av någons dator och att personen känner sig hotad, till att man stänger ner regeringens viktiga webbplatser. Författarna i artikel [1, 3] anser att cyberhot inte är ett hot eftersom dess påföljder inte är märkbara. För att konkret kunna peka fingret på vad som är rätt eller fel måste man först definiera ordet hot. Enligt avgränsningen i uppsatsen är all form av cyber-attack mer eller mindre ett hot där påföljden inte behöver vara en fysisk skadegörelse. Skadegörelsen kan ske i form av att livskrävande system stängs ner och i sin följd kan kräva ett eller annat liv.

Utifrån bland annat tabellen (*Tabell 1*) kan man se att hela sex av åtta publikationer relaterar cyberkrig med verkligt hot mot både samhällsfunktioner men även Statsmakter. Med brett stöd utifrån artiklar och publikationer som återfinns i uppsatsen kan man därmed dra slutsatsen ja, cyberkrig är ett reallt hot mot våra samhällsfunktioner och bör tas på största allvar.

(*Tabell 1*)

<b>Publikationer</b>	<b>Anser att cyberkrig är ett hot</b>
Publikation A	Nej
Publikation B	Nej
Publikation C	Ja
Publikation D	Ja
Publikation E	Ja
Publikation F	Ja
Publikation G	Ja
Publikation H	Ja

## 10. Referenslista

### Publikationer:

[1] "Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats", James A. Lewis, Center for Strategic and International Studies, December 2002

[http://csis.org/files/media/isis/pubs/021101\\_risks\\_of\\_cyberterror.pdf](http://csis.org/files/media/isis/pubs/021101_risks_of_cyberterror.pdf)

[2] "Cyberwar Thresholds and Effects", James A. Lewis, Center for strategic and International Studies, September/October 2011

<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05719593>

[3] "Cyber war will not take place", Thomas Rid, 05- October 2011

<http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939>

[4] "Cyber war will take place!", John Stone, The Journal of Strategic Studies, 2013

<http://www.tandfonline.com/doi/pdf/10.1080/01402390.2012.730485>

[5] "Cyber-attacks seem Meant to Destroy, Not Just Disrupt", Nicole Perlroth and David E. Sanger, The New York Times, March 28-2013

<http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-look-to-destroy-data.html?pagewanted=all>

[6] "Panetta Warns of Dire Threat of Cyber-attack on U.S. ", Elisabeth Bumiller and Thom Shanker, The New York Times, October 11-2012

<http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all>

[7] "Obama Order sped up wave of Cyber-attacks against Iran", David E Sanger, the New York Times, June 1-2012

<http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all>

[8] "ATM thieves conducted massive cyber-attack", Zachary A. Goldfarb, the Washington Post, May 09-2013

[http://articles.washingtonpost.com/2013-05-09/business/39142997\\_1\\_prepaid-debit-cards-heist-gift-cards](http://articles.washingtonpost.com/2013-05-09/business/39142997_1_prepaid-debit-cards-heist-gift-cards)

Trost, J., (2005): *Kvalitativa intervjuer*. Studentlitteratur, Lund.

## Internet:

Bild 1: <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>

[9] Publikation: "*Significant Cyber Events*", James Andrew Lewis  
[http://csis.org/files/publication/120504\\_Significant\\_Cyber\\_Incidents\\_Since\\_2006.pdf](http://csis.org/files/publication/120504_Significant_Cyber_Incidents_Since_2006.pdf)

[10] Publikation: "*What Is a Cyber-Attack*", Harpreet, 2011-2012  
<http://www.trivology.com/articles/297/what-is-a-cyber-attack.html>

[11] Publikation: "*What is a Cyber-Attack*", Malcom Tatum, 2014  
<http://www.wisegeek.com/what-is-a-cyberattack.htm>

[12] Publikation: "*Cyberattack*", Dictionary.com, 2014  
<http://dictionary.reference.com/browse/cyberattack>

[13] Publikation: "*Will cyberattacks define the future of war*", Taylor Armerding, 2012  
<http://www.csoonline.com/article/715128/will-cyberattacks-define-the-future-of-war->

[14] Publikation: "*Cyberattack*", Cory Janssen, 2010-2014  
<http://www.techopedia.com/definition/24748/cyberattack>

[15] Publikation: "*Cyber Threat Source Descriptions*",  
Government Accountability Office (GAO), 2005  
<http://ics-cert.us-cert.gov/csthreats.html>

[16] Publikation: "*What is Cyberwar*", Mary McMahon, 2014  
<http://www.wisegeek.com/what-is-cyberwar.htm>

[17] Publikation: "*What is Cyberwarfare?*", Secpoint, 1999-2014  
<http://www.secpoint.com/what-is-cyberwarfare.html>

[18] Publikation: "*What is Cyber Warfare?*", Brendan McGuigan, 2014  
<http://www.wisegeek.com/what-is-cyber-warfare.htm>

[19] Publikation: "*What is Cyberwarfare?*", Cory Janssen, 2010-2014  
<http://www.techopedia.com/definition/13600/cyberwarfare>

[20] Publikation: "*What is a Hacker?*", Bradley Mitchell, 2009  
<http://compnetworking.about.com/od/networksecurityprivacy/f/what-is-hacking.htm>

[21] Publikation: "*What is a Hacker?*", Garry Crystal, 2014  
<http://www.wisegeek.org/what-is-a-hacker.htm>

[22] Publikation: "*Attack mot svenska hemsidor*", Per Nygren, 2012  
<http://www.gp.se/nyheter/sverige/1.1085952-attack-mot-svenska-hemsidor>

- [23] Publikation: "*The Real Story of Stuxnet*", David Kushner, 2013  
<http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>
- [24] Publikation: "*Stuxnet Attack on Iran was Illegal Act of force*", Kim Zetter, 2013  
<http://www.wired.com/threatlevel/2013/03/stuxnet-act-of-force/>
- [25] Publikation: "*Cyberattacks Seem Meant to Destroy, Not Just Disrupt*", Nicole Perlroth and David E. Sanger, 2013  
[http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-look-to-destroy-data.html?\\_r=0](http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-look-to-destroy-data.html?_r=0)
- [26] Publikation: "*Iran denies hacking into American banks*", Zahra Hosseinian, 2012  
<http://www.reuters.com/article/2012/09/23/us-iran-cyberattacks-denial-idUSBRE88M06O20120923>
- [27] Publikation: "*Guide to Industrial Control Systems (ICS) Security*", Keith Stouffer, Joe Falco, Karen Scarfone, 2011  
<http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf>
- [28] Publikation: "*Google Still World's Most Popular Search Engine By Far, But Share Of Unique Searchers Dips Slightly*", Danny Sullivan, 2013  
<http://searchengineland.com/google-worlds-most-popular-search-engine-148089>
- [29] Publikation: "*Desktop Search Engine Market Share*", Netmarketshare, 2014  
<https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0>
- [30] Publikation: "*Worldwide internet user's reaches 2bn*", 2011  
<http://www.news.com.au/technology/worldwide-internet-users-reaches-2bn/story-e6frfro0-1225995328284>
- [31] Publikation: "*We're becoming gadget hoarders: Sophos*", Nermin Bajric, 2013  
[http://www.arnnet.com.au/article/456450/we\\_re\\_becoming\\_gadget\\_hoarders\\_sophos/](http://www.arnnet.com.au/article/456450/we_re_becoming_gadget_hoarders_sophos/)
- [32] Publikation: "*Taking a (Virtual) Break: Can You Survive Without Your Technology for 24 Hours? I Doubt it!*", Larry Rosen, 2010  
<http://www.psychologytoday.com/blog/rewired-the-psychology-technology/201010/taking-virtual-break-can-you-survive-without-your-tech>
- [33] Publikation: "*Technology Use around the World*", 2011  
<http://www.pewresearch.org/daily-number/technology-use-around-the-world/>
- [34] Publikation: "*Usage Statistics: Pew Internet Releases Teens and Technology 2013*", Gary Price, 2013  
<http://www.infodocket.com/2013/03/13/usage-statistics-pew-internet-releases-teens-and-technology-2013/>

- [35] Publikation: ”*Technology now and expectation in daily life*”, Intel Free Press, 2012  
<http://www.intelfreepress.com/news/technology-now-an-expectation-in-daily-life/2231>
- [36] Publikation: “*Technology lowers our expectations of others, Turkle says*”, Rebecca Myers, 2012  
<http://chqdaily.com/2012/07/29/technology-lowers-our-expectations-of-others-turkle-says/>
- [37] Publikation: “*Consumer expectations changing alarm technology*”, Joel Griffin, 2013  
<http://www.securityinfowatch.com/article/10915068/consumer-expectations-changing-alarm-technology>
- [38] Publikation: ”*Technology now and expectation in daily life*”, Intel Free Press, 2012  
<http://www.intelfreepress.com/news/technology-now-an-expectation-in-daily-life/2231>
- [39] Publikation: “*Internet History timeline: Arpanet to the World Wide Web*”; Kim Ann Zimmermann, 2012  
<http://www.livescience.com/20727-internet-history.html>
- [40] Publikation: ”*Internet History*”, Computer History Museum, 2004  
[http://www.computerhistory.org/internet\\_history/](http://www.computerhistory.org/internet_history/)
- [41] Publikation: “*A Technical History of the ARPANET - A Technical Tour*”, Dr. Edmundson-Yurkanon, 2001  
<http://www.cs.utexas.edu/users/chris/nph/ARPANET/ScottR/arpanet/tour/overview.htm>
- [42] Publikation: ”*A Brief History of the Internet*”, Robert H Zakon, 2012  
<http://walthowe.com/navnet/history.html>
- [43] Publikation: ”*The history of computers, networks and modems*”, Ian Peter, 2004  
<http://www.nethistory.info/History%20of%20the%20Internet/netsnmods.html>
- [44] Publikation: ”*History of the Internet*”, NewMedia  
<http://www.newmedia.org/history-of-the-internet.html>
- [45] Publikation: ”*History of the Internet*”, InetDaemon, 2013  
<http://www.inetdaemon.com/tutorials/internet/history.shtml>
- [47] Publikation: “*Boundless Informant: the NSA's secret tool to track global surveillance data*”, Glenn Greenwald, Ewen MacAskill, 2013  
<http://www.guardian.co.uk/world/2013/jun/08/nsa-boundless-informant-global-datamining>
- [48] Publikation: “*Hemlig lista visar USA:s övervakning*”, Dn.se, 2013  
<http://www.dn.se/ekonomi/hemlig-lista-visar-usas-overvakning/>

- [49] Publikation: ”*Europeisk oro för USA:s internetövervakning*”, Fredrik Haglund, 2013  
<http://www.europaportalen.se/2013/06/europeisk-oro-for-usas-internetovervakning>
- [50] Publikation: ”*US and Germany to hold talks over European NSA surveillance concerns*”, Dan Roberts, 2013  
<http://www.guardian.co.uk/world/2013/jul/04/usa-germany-obama-merkel-talks-nsa>
- [51] Publikation: ”*Should Big Brother’s Surveillance Comfort or Scare Us?*”, Patricia Zengerle, Tabassum Zakaria, 2013  
<http://www.charismanews.com/us/39919-should-big-brother-s-surveillance-comfort-or-scare-us>
- [52] Publikation: ”*In worldwide surveillance age, US has big edge*”, Raphael Satter, 2013  
<http://phys.org/news/2013-07-golden-age-surveillance-big-edge.html>
- [54] Publikation: ”*Snowden reveals Microsoft granted NSA access to Outlook, SkyDrive and Skype*”, The Voice of Russia, 2013  
[http://english.ruvr.ru/news/2013\\_07\\_12/Microsoft-granted-secret-services-access-to-Outlook-SkyDrive-and-Skype-1324/](http://english.ruvr.ru/news/2013_07_12/Microsoft-granted-secret-services-access-to-Outlook-SkyDrive-and-Skype-1324/)
- [55] Publikation: ”*Obama administration defends 2<sup>nd</sup> mass surveillance project*”, FoxNews, 2013  
<http://www.foxnews.com/politics/2013/06/07/intelligence-officials-reportedly-mining-data-from-us-internet-companies/>
- [56] Publikation: ”*Is UK doing enough to protect itself from cyber attack*”, Mark Urban, 2013  
<http://www.bbc.co.uk/news/uk-22338204>
- [57] Publikation: ”*Is your business ready for Cyber War?*”, Julie Cohn, 2013  
<http://www.cnbc.com/id/100449619>
- [58] Publikation: ”*Estonia trains army of experts to protect itself from cyber attacks*”, Daily Mail Reporter, 2011  
<http://www.dailymail.co.uk/sciencetech/article-1344402/Estonia-trains-army-experts-protect-cyber-attacks.html>
- [59] Publikation: ”*Preparing for cyberwarfare*”, Michael Richardson, 2013  
<http://www.japantimes.co.jp/opinion/2013/07/03/commentary/preparing-for-cyberwarfare/#.Ue3D2W37ZNY>
- [60] Publikation: ”*5 ways to fight back against Cyber attack*”, The Week, 2013  
<http://theweek.com/article/index/243112/5-ways-to-fight-back-against-chinese-cyber-attacks>
- [61] Publikation: ”*Recent Cyber Attacks*”, Forbes  
<http://www.forbes.com/pictures/mhl45gkeg/sony-2/>

[62] Publikation: *"China Cyber Attacks: A Reminder to Strengthen U.S. Cyber Defense"*, Pierce Stanley, 2013

<http://www.policymic.com/articles/27111/china-cyber-attacks-a-reminder-to-strengthen-u-s-cyber-defense>

[63] Publikation: *"Cyberattacks against U.S. Corporations are on the rise"*, David E. Sanger, Nicole Perloth, 2013

<http://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html?pagewanted=all&r=0>

[64] Publikation: *"Cyber attacks against banks more severe than most realize"*, Joseph Menn, 2013

<http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518>

[65] Publikation: *"Are we becoming too dependent on the internet"*, Robert Harrison, 2012

<http://www.austin-williams.com/blog/post.cfm/are-we-becoming-too-dependent-on-the-internet>

[66] Publikation: *"An ugly toll of technology: Impatience and Forgetfulness"*, Tara Parker Pope, 2010

<http://www.nytimes.com/2010/06/07/technology/07brainside.html>

[67] Publikation: *"Companies think they're prepared for APT cyber attacks, but they aren't"*, Ted Samson, 2013

<http://www.infoworld.com/t/security/companies-think-theyre-prepared-apt-cyberattacks-they-arent-212796>

[68] Publikation: *"Cyberattacks mean big business for small security firms"*, Cadie Thompson, 2013

<http://www.cnbc.com/id/100777039>

[69] Publikation: *"Iran-Based hackers traced to cyber attack on U.S. company"* Chris Strohm, 2013

<http://www.businessweek.com/news/2013-05-14/iran-based-hackers-traced-to-cyber-attack-on-company-inside-u-dot-s-dot>

[70] Publikation: *"As cyber threats mount, business is booming in the security world"*, Matt Egan, 2013

<http://www.foxbusiness.com/technology/2013/03/12/as-cyber-threats-mount-business-is-booming-in-security-world/>

[71] Publikation: *"The U.S. outsources Cybersecurity & Defense to contractors that keep getting hacked"*, Andrea Peterson, 2013

<http://thinkprogress.org/security/2013/05/03/1958871/contractors-outsource-cybersecurity-hacked/?mobile=nc>

[72] Publikation: "New Report underestimates number of Chinese cyber attacks", Jason Koebler, 2013

<http://www.usnews.com/news/articles/2013/02/19/experts-new-report-underestimates-number-of-chinese-cyber-attacks>

[73] Publikation: "Your business is never too small for a cyber attack, here's how to protect yourself", Forbes, 2013

<http://www.forbes.com/sites/forbesleadershipforum/2013/05/13/your-business-is-never-too-small-for-a-cyber-attack-heres-how-to-protect-yourself/>

[74] Publikation: "Security alliance plans to improve resilience against cyber attack", David Bicknell, 2013

<http://central-government.governmentcomputing.com/news/security-alliance-plans-to-improve-resilience-against-cyber-attack>

[75] Publikation: "Snowden: US and Israel did create Stuxnet attack code", Iain Thomson, 2013

[http://www.theregister.co.uk/2013/07/08/snowden\\_us\\_israel\\_stuxnet/](http://www.theregister.co.uk/2013/07/08/snowden_us_israel_stuxnet/)

[76] Publikation: "The Real Story of Stuxnet", David Kushner, 2013

<http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>

[77] Publikation: "Snowden confirms NSA created Stuxnet with Israeli aid", Thomas Peter, 2013

<http://rt.com/news/snowden-nsa-interview-surveillance-831/>

[78] Publikation: "Biometric hacking team uses photographed fingerprint to get past touch id", Scott Buscemi, 2013

<http://9to5mac.com/2013/09/22/biometrics-hacking-team-uses-photographed-fingerprint-to-get-past-touch-id/>

[79] Publikation: "Nytt försäljningsrekord för iPhone med över nio miljoner sålda enheter första helgen", Petter Ahrnstedt, 2013

<http://www.apple.com/se/pr/library/2013/09/23First-Weekend-iPhone-Sales-Top-Nine-Million-Sets-New-Record.html>

[80] Publikation: "Samsung har sålt 38 miljoner telefoner i Note-Serien", Jon Fingas, 2013

<http://www.swedroid.se/samsung-har-salt-38-miljoner-telefoner-i-note-serien/>

[81] Publikation: "iPhone 5 säljer bättre än Galaxy SIII", Mikael Markander, 2013

<http://macworld.idg.se/2.1038/1.493403/iphone-5-saljer-battre-an-galaxy-s-iii>

[82] Publikation: "Fem skäl att sats på ökad automatisering", Stefan Nordberg, 2012

<http://www.nyteknik.se/nyheter/automation/verkstadsautomation/article3471183.ece>

[83] Publikation: "Säkra system kräver automatisering", Kent Olofsson, 2013

<http://sakerhet24.idg.se/2.29373/1.523127/sakra-system-kraver-automatisering>

[84] Publikation: *"Hacker hits on U.S. power and nuclear targets spiked in 2012"*, David Goldman, 2013

<http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/>

[85] Publikation: *"Cyber Incident Blamed for Nuclear Power Plant Shutdown"*, Brian Krebs, 2008

<http://www.waterfall-security.com/cyber-incident-blamed-for-nuclear-power-plant-shutdown-june-08/>

[86] Publikation: *"Call of the Wild: 7 strange smartphone habits"*, Catey Hill, 2012

<http://www.forbes.com/sites/cateyhill/2012/07/24/call-of-the-wild-7-strange-smartphone-habits/>

[87] Publikation: *"Do you obsessively check your Smartphone"*, Elizabeth Cohen, 2011

<http://edition.cnn.com/2011/HEALTH/07/28/ep.smartphone.obsessed.cohen/>

[88] Publikation: *"Do we rely too much on computers?"*, BBC NEWS – Talking point, 2000

[http://news.bbc.co.uk/2/hi/talking\\_point/703939.stm](http://news.bbc.co.uk/2/hi/talking_point/703939.stm)

[89] Publikation: *"Combating cyber threats to national security"*, John P. Carlin

<http://www.justice.gov/nsd/combatacyberthreats.html>

[90] Publikation: *"FBI director warns of cyberattacks, other security chiefs say terrorism threat has altered"*, Greg Miller, 2013

[http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0\\_story.html](http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html)

[91] Publikation: *"Bank seek U.S. help on Iran cyberattacks"*, Siobhan Gorman, Danny Yadron, 2013

<http://online.wsj.com/news/articles/SB10001424127887324734904578244302923178548>

[92] Publikation: *"Cyber attack, war game tests London banks"*, Matt Scuffham, Joshua Franklin, 2013

<http://in.reuters.com/article/2013/11/12/banks-wargame-idINDEE9AB00120131112>

[93] Publikation: *"Every minute of every day a bank is under cyber attack"*, Harry Wilson, 2013

<http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/10359563/Every-minute-of-every-day-a-bank-is-under-cyber-attack.html>

[94] Publikation: *"Are you prepared? Record number of cyber attacks target small business"*, Cheryl Conner, 2013

<http://www.forbes.com/sites/cherylsnappconner/2013/09/14/are-you-prepared-71-of-cyber-attacks-hit-small-business/>

[95] Publikation: *"An emerging target for cyber attacks: Trust"*, William Jackson, 2013

<http://gcn.com/blogs/cybereye/2013/01/trust-infrastructure-top-cyber-targets.aspx>

[96] Publikation: *"Banks, Utilities seen as targets of Syrian cyber attacks"*, Michael Riley, Chros Strohm , 2013

<http://www.bloomberg.com/news/2013-08-28/banks-utilities-seen-as-targets-of-syrian-cyber-attacks.html>

[97] Publikation: *"Obama orders US to draw up overseas target list for cyber attacks"*, Gleen Greenwald, Ewen MacAskill, 2013

<http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas>

[98] Publikation: *"Home users face growing risk och cyber attack"*, Jennifer LeClaire, 2006

<http://www.technewsworld.com/story/53213.html>

[99] Publikation: *"Cyber Attack"*; Ready, 2013

<http://www.ready.gov/cyber-attack>

[100] Publikation: *"Protect myself from cyber attacks"*, Homeland Security

<http://www.dhs.gov/how-do-i/protect-myself-cyber-attacks>

[101] Publikation: *"30 years of risky business: A cybersecurity timeline"*; GCN Staff, 2013

<http://gcn.com/articles/2013/05/30/gcn30-timeline-cybersecurity.aspx>

[102] Publikation: *"Cyberwar Timeline: The roots of this increasingly menacing challenge facing nations and businesses"*, Beth Rowen

<http://www.infoplease.com/world/events/cyberwar-timeline.html#1990>