ISSN (e): **2250 – 3005** || Volume, 07 || Issue, 08|| August – 2017 ||
International Journal of Computational Engineering Research (IJCER)

Challenges in Cybersecurity

[1]SAMARENDRA SAMAL, [2]SOUMYA RANJAN PATTANAIK,
Gandhi Institute of Excellent Technocrats, Bhubaneswar, India
Kalam Institute of Technology,Berhampur, Ganjam, Odisha, India

INTRODUCTION

Informationhasbeenconsideredasignificantaspectof **power**, diplomacy, and armed conflict for a verylongtime.Sincethe1990s,however,information'sroleininternationalrelationsandsecurityhasdiversifiedand its importance for political matters has increased,mostly due to the proliferation of **information andcommunication technology (ICT)** into all aspectsoflifeinpost-industrializedsocieties.Theabilitytomaster the generation, management, use but also ma-nipulation of information has become a desired powerresource since the control over knowledge, beliefs,andideasareincreasinglyregardedasacomplementto control over tangible resources such as militaryforces, raw materials, and economic productive capa-bility. Consequently, matters of cyber-(in)-security—althoughnotalwaysunderthisname—havebecomeasecurityissue.
Inthischapter,thecyber-(in)-securitylogicisun-packedinfoursectionsasdescribedintheReader'sGuide, with the first providing the necessary technicalbackgroundinformationonwhytheinformationin-frastructure is inherently insecure, how computer vul-nerabilities are conceptualized, who can exploit themandinwhatways.

Informationsecurity101

Cyberspace connotes the fusion of all communica-tion networks, databases, and sources ofinformationinto a vast, tangled, and diverse blanket of electronicinterchange. A 'network ecosystem' is created; it isvirtualandit'existseverywherethereаretelephonewires, coaxial cables, fi bre-optic lines or electromag-neticwaves'(Dysonetal.1996).Cyberspace,how-ever, is not only virtual, since it is also made up ofservers,cables,computers,satellites,etc.Inpopularusage we tend to use the terms cyberspace and **In-ternet**almost interchangeably, even though the In-ternet,albeitthemostimportantone,isjustonepartofcyberspace.
Cyber-security is both about the insecurity createdby and through this new place/space and about thepracticesorprocessestomakeit(more)secure.Itre-fers to a set of activities and measures, both technicalandnon-technical,intendedtoprotectthebioelectri-cal environment and the data it contains and trans-portsfromallpossiblethreats.

Theinherentinsecurityofcomputernetworks

Today's version of the Internet is a dynamic evolu-tion of the Advanced Research Projects Agency Net-work (ARPANET), which was mainly designed foroptimized information exchange between the uni-versities and research laboratories involved in UnitedStates Department of Defense (DoD) research. At thetime,therewasnoapparentneedforaspecificfocuson security, because information systems were beinghostedonlargeproprietarymachinesthatwerecon-nected to very few other computers. Therefore, thenetwork designers emphasized robustness and surviv-abilityoversecurity.
DuetothedynamicevolutionofARPANET,thisturned into a legacy problem. What makes systemsso vulnerable today is the confluence of the samebasic network technology (not built with security inmind), the shift to smaller and far more open systems(not built with security in mind), and the rise of ex-tensivenetworkingatthesametime.Inaddition,thecommercializationoftheInternetinthe1990sledtoanevenbiggersecuritydeficit.Therearesignificantmarket-driven obstacles to IT-security: there is nodirectreturnoninvestment,time-to-marketimpedesextensive security measures, and security mecha-nismshaveanegativeimpactonusabilitysothatse-curity is often sacrificed for functionality (AndersonandMoore2006).
There are additional forces keeping cyberspaceinsecure: **Big Data** is considered the key IT trend ofthefuture,andcompanieswanttousethemassesofdata that we produce every day to tailor theirmarketingstrategiesthroughpersonalizedadvertis-ing and prediction offuture consumer behaviour.Therefore, there is little interest in encrypted (andthereforesecure)informationexchange.Ontopof this, the intelligence agencies of this world havethe same interest in data that can be easily grabbedandanalysed.Furthermore,the**NSA-revelationsof2013**haveexposedthatintelligenceservicesare making cyberspace more insecure directly—inordertobeabletohavemoreaccesstodata,andin order to prepare for future cyber-conflict, theybuyandexploitso-called**zero-dayvulnerabilities**in current operating systems and hardware to in-jectmalwareintonumerousstrategicallyoppor-tunepointsoftheInternetinfrastructure(DunnCavelty2014).

Computervulnerabilitiesandthreatagents

The terminology in information security is oftenseemingly congruent with the terminology in na-tionalsecuritydiscourses:itisaboutthreats,agents,vulnerabilities,etc.However,thetermshaveveryspe-cific meanings so that seemingly clear analogies mustbeusedwithcare.Themainfocusofthecyber-secu-rity discourse are information attacks (both passiveand active), defined as (potentially) damaging eventsorchestratedbyahumanadversary('threatagents').The most common label bestowed upon them is**hacker** (Erickson 2003). For members of the com-puting community, 'hacker' describes a member ofa distinct social group (or sub-culture); a particularlyskilled programmer or technical expert who knowsaprogramminginterfacewellenoughtowritenovelsoftware. A particular ethic is ascribed to this subcul-ture:abeliefinsharing,openness,andfreeaccesstocomputersandinformation;decentralizationofgov-ernment; and in improvement of the quality of life(Levy 1984). In popular usage and in the media, how-ever, the term hacker generally describes computerintrudersorcriminals.

In the cyber-security debate, hacking is consideredamodusoperandithatcanbeusednotonlybytech-nologically skilled individuals for minor misdemean-ours, but also by organized actor groups with trulybad intent, such as terrorists or foreign states. Somefew hackers have the skills to attack those parts ofthe information infrastructure considered 'critical'for the functioning of society. Although most peoplewould lack the motivation to cause violence or severeeconomic or social harm, government officials fearthat individuals with the capability to cause seriousdamage could be swayed and corrupted by monetaryincentives.

Hackingtools

Thetermusedforthetoolsofacyber-attackis**mal-ware**(malicious+software).Well-knownexamplesarevirusesandworms,computerprogramsthatrep-licate functional copies of themselves with varyingeffectsrangingfrommereannoyanceandinconven-ience to compromise of the confidentiality or integrityofinformation.TherearealsoTrojanhorses,programsthat masquerade as benign applications but set up abackdoorsothatthehackercanreturnlaterandenter

the system. Often system intrusion is the main goal ofmoreadvancedattacks:iftheintrudergainsfullsys-tem control, or 'root' access, he has unrestricted ac-cess to the inner workings of the system (Anonymous2003). Due to the characteristics of digitally storedinformation an intruder can delay, disrupt, corrupt,exploit, destroy, steal, and modify information. De-pending on the value of the information or the impor-tanceoftheapplicationforwhichthisinformationisrequired, such actions will have different impacts withvaryingdegreesofgravity.

KEYPOINTS

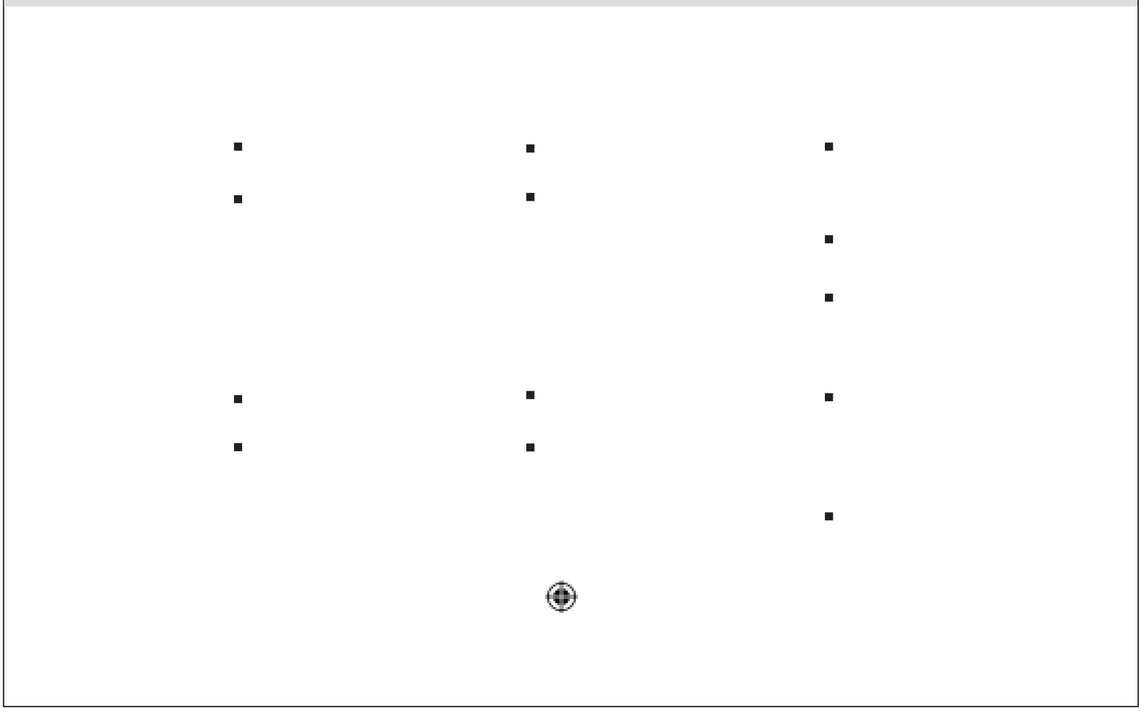
- Cyberspacehas both virtual and physical elements. WetendtousethetermscyberspaceandInternetinterchangeably,eventhoughcyberspaceencompassesfarmorethanjust theInternet.
- Cyber-securityisbothabouttheinsecuritycreatedthroughcyberspaceandaboutthetechnicalandnon-technicalpracticesofmakingit(more)secure.
- The Internet started as ARPANET in the 1960s and wasneverbuiltwithsecurityinmind.Thislegacy,combinedwiththerapidgrowthofthenetwork,itscommercializa-tion, and several economic and strategic interests makecomputernetworks inherentlyinsecure.
- Information security uses avocabulary very similartonationalsecuritylanguage,buthasspecificmeanings.Cyber-attacks are themain focus ofthe cyber-securitydiscourse.Attackersarecalledhackers.
- The umbrella term for all hacker tools is malware. Themaingoalofadvancedattacksisfullsystemcontrol,whichallowstheintrudertodelay,disrupt,corrupt,exploit,destroy,steal,ormodifyinformation.

Three interlocking cyber-securitydiscourses

The cyber-security discourse originated in the USAin the 1970s, built momentum in the late 1980s andspread to other countries in the late 1990s. The USgovernment shaped both the threat perception andthe envisaged countermeasures with only little vari-ationinothercountries.Ontheonehand,thedebatewas decisively influenced by the larger post-Cold Warstrategic context in which the notion of asymmetricvulnerabilities, epitomized by the multiplication ofmaliciousactors(bothstateandnon-state)andtheirincreasing capabilities to do harm, started to play akey role. On the other hand, discussions about cyber-security always were and still are influenced by theongoing**informationrevolution**,whichtheUSAisshaping both technologically and intellectually by dis-cussing its implications for international relations andsecurityandactingontheseassumptions.

Thecyber-securitydiscoursewasneverstaticbe-cause the technical aspects of the information infra-structureareconstantlyevolving.Mostimportantly,changes in the technical sub-structure changed thereferentobject.Inthe1970sand1980s,cyber-securitywasaboutthosepartsoftheprivatesectorthatwerebecoming digitalized and also about government net-worksandtheclassifiedinformationresidinginit.Thegrowth and spread of computer networks into moreand more aspects of life changed this limited referentobject in crucial ways. In the mid-1990s, it becameclear that key sectors of modern society, includingthose vital to national security and to the essentialfunctioning of (post-)industrialized economies, hadcometorelyonaspectrumofhighlyinterdependentnational and international software-based control sys-tems for their smooth, reliable, and continuous opera-tion.Thereferentobjectthatemergedwasthetotality

Figure27.1Threediscourses



of**critical(information)infrastructures**thatprovidethewayoflifethatcharacterizesoursocieties.

Whentellingthecyber-security-storywecandis-tinguish between three different, but often closelyinterrelatedandreinforcingdiscourses,withspecificthreat imaginaries and security practices, referent ob-jects, and key actors. The first is a technical discourseconcerned with malware (viruses, worms, etc.) andsystemintrusions.Thesecondisconcernedwiththephenomena cyber-crime and cyber-espionage. Thethird is a discourse driven initially by the US military,focusingonmattersof**cyber-war**initiallybutincreas-ingly also on **critical infrastructure protection** (seeFigure27.1).

Viruses,worms,andotherbugs(technicaldiscourse)

The technical discourse is focused on computer andnetwork disruptions caused by different types of mal-ware.Asearlyas1988,theARPANEThaditsfirstmajornetwork incident: the ‘Morris Worm’. The worm usedsomanysystemresourcesthattheattackedcomput-ers could no longer function and large parts of theearlyInternetwentdown.Thedevastatingeffectsled

	Technical	**Crime–Espionage**	**Military/civildefence**
Mainactors	Computerexperts Anti-virusindustry	Lawenforcement Intelligencecommunity	Nationalsecurityexperts Military Civil defenceestablishment
Mainreferentobject	Computers Computernetworks	Business networks Classifiedinformation(governmentnetworks)	Military networks,networked armedforces Critical(information)infrastructures

tothesetupofacentretocoordinatecommunicationamong computer experts during IT emergencies: aComputer Emergency Response Team (CERT). Thiscentre, now called the CERT Coordination Center,still plays a considerable role in computer securitytoday and served as a role model for many similarcentres all over the world. Around the same time, theanti-virus industry emerged and with it techniquesandprogramsforvirusrecognition,destruction,andprevention.

The worm also had a substantial psychological im-pact by making people aware just how insecure andunreliable the Internet was. While it had been accept-ableinthe1960sthatpioneeringcomputerprofession-als were hacking and investigating computer systems,thesituationhadchangedbythe1980s.Societyhadbecome dependent on computing in general for busi-ness practices and other basic functions. Tamperingwith computers suddenly meant potentially endan-geringpeople'scareersandproperty;andsomeevensaidtheirlives(Spafford1989).Eversince,malwareas'visible'proofofthepersuasiveinsecurityoftheinfor-mation infrastructure has remained in the limelight ofthecyber-securitydiscourse;anditalsoprovidestheback-story for the other two discourses. Table 27.1listssomeofthemostprominentexamples.

Most obviously, the history of malware is a mir-ror of technological development: the type of mal-ware, the type of targets, and the **attack vectors** allchanged with the technology and the existing techni-cal countermeasures (and continue to do so). This de-velopmentgoesinsyncwiththedevelopmentofthecyber-crime market, which is driven by the huge sumsof money available to criminal enterprises at low riskof prosecution. While there was a tongue-in-cheekquality to many of the viruses in the beginning, vi-ruses have long ago lost their innocence. Even thoughprank-like viruses have not disappeared, computer se-curityprofessionalsareincreasinglyconcernedwiththerisinglevelofprofessionalizationcoupledwiththeobviouscriminal (orevenstrategic)intentbehindat-tacks. Advanced malware is targeted: a hacker picks avictim,scopesthedefences,andthendesignsmalwareto get around them (Symantec 2010). The most prom-inent example for this kind of malware is Stuxnet (seeCase Study 27.2). However, some IT security compa-nies have recently warned against overemphasizingso called **advanced persistent threat** attacks just be-causewehearmoreaboutthem(Verizon2010:16).Onlyabout3percentofallincidentsareconsidered sosophisticatedthattheywereimpossibletostop.Thevastmajorityofattackersgoaftersmalltomedium-sized enterprises with bad defences. These types ofincidents tend to remain under the radar of the mediaandevenlaw-enforcement.

KEYPOINTS

- In 1988, the Morris Worm downed large parts of theearlyInternet,provingthetheoryrightandmakingcleart hattheInternetwasaveryinsecuretechnology.
- As a consequence, the CERT Coordination Center wasfounded. It is still very active today and has served as amodelforsimilarcomputeremergencyresponseteamsinman ycountries.
- There is a long list of prominent malware which oftenmade headlines. Over the years, malware has becomemore sophisticated and more clearly linked to criminalintent.
- The mostdangerous malwareistailored toa specifictargetforhigheffect.However,thelargemajorityofat-tacks remains fairly unsophisticated and go after small ormedium-sized enterprises withlittle IT securityawarenessand/orinvestment.

Cyber-crooksanddigitalspies(crime-espionagediscourse)

The cyber-crime discourse and the technical discourseareverycloselyrelated.ThedevelopmentofITlaw(and,morespecifically,Internetorcyber-law)indiffer-entcountriesplaysacrucialroleintheseconddiscoursebecauseitallowsthedefinitionandprosecutionofmis-demeanour.Notsurprisingly,thedevelopmentoflegaltools to prosecute unauthorized entry into computersystemscoincidedwiththefirstseriousnetworkinci-dentsdescribedhere(cf.MungoandClough1993).

Cyber-crime has come to refer to any crime thatinvolves computers and networks, like a release ofmalware or spam, fraud, and many other things. Untiltoday,notionsofcomputer-relatedeconomiccrimesdetermine the discussion about computer misuse.However,adistinctnational-securitydimensionwasestablished when computer intrusions (a criminal act)were clustered together with the more traditionaland well-established espionage discourse. Prominenthackingincidents—suchastheintrusionsintohigh-level computers perpetrated by the Milwaukee-based‘414s’—ledtoafeelinginpolicycirclesthattherewas

Customer	BookTitle	Stage	Supplier	Date
OUP	ContemporarySecurityStudies,4e	FirstProof	ThomsonDigital	28 Aug2015

Table27.1Prominentmalware

Nameof malware	Yearof discovery	Creator	Infected	Effect
MorrisWorm	1988	Robert Morris(computer student),USA	UNIXsystems	SloweddownmachinesintheARPANETuntilthey becameunusable Huge impact on thegeneral awareness ofinsecurity
Michelangelo	1992	(unknown)	DOSsystems	Overwrotethefirsthundredsectorsoftheharddisk withnulls Causedfirstdigitalmasshysteria
BackOrifice	1998	CultoftheDeadCow (hackercollective),USA	Windows98	Toolforremotesystemadministration(Trojanhorse)
Melissa	1999	DavidL.Smith (programmer),USA	MicrosoftWord, Outlook	ShutdownInternetmail,cloggedsystemswith infectede-mails
ILoveYou	2000	ReomelRamoresandOnel	Windows	Overwrotefileswithcopyofitself,sentitselftothe

		deGuzman(computer students),Philippines		firstfiftypeopleintheWindowsAddressBook
CodeRed	2001	(unknown)	Microsoftweb servers	Defacedwebsites,usedmachinesforDDoS-attacks
Nimda	2001	(unknown)	Windows workstationsand servers	Allowedexternalcontroloverinfectedcomputers
Blaster	2003	JeffreyLeeParson (18-year-oldstudent), USA	WindowsXPand 2000	DDos-attacksagainst'windowsupdate.com' Sideeffects:systemcrash.Wassuspectedtohave causedblack-outinUSA(couldnotbeconfirmed)
Slammer	2003	(unknown)	Windows95–XP	DDoS-attacks,sloweddownInternettraffic worldwide
Sasser	2004	SvenJaschan(computer science student), Germany	WindowsXPand Windows2000	Internettrafficslowdown,systemcrash
Zeus	2007	(unknown),availableto buyinunderground computerforums	Windows	Stealsbankingandotherinformation,formsbotnets
Conficker (several versions)	2008	(unknown)	Windows	Formsbotnets
Stuxnet	2010	AttributedtoUSand Israeligovernment (OperationOlympic Games)	SCADA system (Siemensindustrial softwareand equipment)	Spieson and subverts industrial systems
Duqu	2011	(unknown)	Windows	Looksforinformationusefulinattackingindustrial controlsystems CodealmostidenticaltoStuxnet(copy-catsoftware)
Flame	2012	AttributedtoUSandIsraeli government(Operation OlympicGames)	Windows	Cyber-espionage(mainlyintheMiddleEast)
Regin	2014	Unknown,probablyNSA AlsousedbyBritish intelligenceagencyGCHQ	Windows	Targeteddatacollection

aneedforaction(Ross1991):ifteenagerswereableto penetrate computer networks that easily, it wasassumed that better organized entities such as stateswould be even better equipped to do so. Other events,like the Cuckoo's Egg incident, the Rome Lab inci-dent,SolarSunrise,orMoonlightMazemadeappar-ent that the threat was not just one of criminals orjuveniles,butthatclassifiedorsensitiveinformationcouldbeacquiredrelativelyeasilybyforeignnationalsthroughhackers(seeTable27.2).

The so-called **attribution problem**—which referstothedifficultyinclearlydeterminingthoseinitiallyresponsible for a cyber-attack plus identifying theirmotivating factors—is the big challenge in the cyber-domain. Due to the architecture of cyberspace, onlineidentities can be optimally hidden. Blame on the basisofthe'cuibono'-logic(whichtranslatesinto'towhosebenefit?') is not sufficient prooffor political action. At-tacks and exploits that seemingly benefit states mightwell be the work of third-party actors operating underavarietyofmotivations.Atthesametime,thechal-lenges of clearly identifying perpetrators also givesstateactorsconvenient'plausibledeniabilityandtheability to officially distance themselves from attacks'(DeibertandRohozinski2009:12).

There are three trends worth mentioning. First,tech-savvy individuals (often juveniles) with the goalofmischieforpersonalenrichmentshapedtheearlyhistory of cyber-crime. Today, professionals dominatethefield.TheInternetisanearidealplaygroundforsemi-andorganizedcrimeinactivitiessuchastheft(like looting online banks, intellectual property, oridentities) or for fraud, forgery, extortion, and **moneylaundering**. Actors in the 'cyber-crime black market'are highly organized regarding strategic and opera-tional vision, logistics, and deployment. Like manyrealcompanies,theyoperateacrosstheglobe.

Second, the cyber-espionage story has changed.Formanyyears,therehasbeenanincreaseinallega-tionsthatChinaisresponsibleforhigh-levelpenetra-tionsofgovernmentandbusinesscomputersystemsin Europe, North America, and Asia. Because Chineseauthoritieshavestatedrepeatedlythattheyconsidercyberspace a strategic domain and that they hope thatmastering it will equalize the existing military imbal-ance between China and the USA more quickly, manyofficialsreadilyaccusetheChinesegovernmentofde-liberateandtargetedattacksorintelligencegatheringoperations.However,theseallegationsalmostexclu-sivelyrelyonanecdotalandcircumstantialevidence.

Furthermore, the NSA revelations in 2013 by EdwardSnowdenhavemadeclearhowmassivethedatacollec-tionbyWesterngovernmentsthroughcyberspaceforstrategicinformationgatheringisandhavegiventhecyber-espionagediscourseanewdirection.

Thethirdtrendistheincreasedattentionthat**hacktivism**—thecombinationofhackingandactivism—has gained in recent years. WikiLeaks,forexample,hasaddedyetanothertwisttothecyber-espionagediscourse.Actingunderthehacker-maxim‘allinformation should be free’, this type of activism delib-eratelychallengestheself-proclaimedpowerofstatestokeepinformation,whichtheythinkcouldendangerordamagenationalsecurity,secret.Itemergesa sacyber-securityissueingovernmentdiscoursebecauseofthewayalotofthedatahasbeenstolen(indigitalform)butalsohowitismadeav ailabletothewholeworldthroughmultiple mirrors (Internet sites). Somewhat related arethemultifacetedactivitiesofhackercollectivessuchasAnonymousorLulzSec.Theycreativelyplaywithano-nymityinatimeobsessedwithcontrolandsurveillanceandhumiliatehigh-visibilitytargetsby**DDoS-attacks**,break-ins,andthereleaseofsensitiveinformation.Fur-thermore, it seems more and more governments areaccepting,ifnotsponsoring,hacktivistactivities.

KEYPOINTS

- Thenotionofcomputercrimeandthedevelopmentof cyber law coincided with the first network attacks.Althoughthisdiscourseismainlydrivenbyeconomicconsiderationsuntiltoday,politicalcyber-espionage,asa specifictypeofcriminalcomputeractivity,startedworry-ingofficialsaroundthesametime.
- Overtheyears,cyber-criminalshavebecomewell-organ-izedprofessionals,operatinginaconsolidatedcyber-crimeblackmarket.
- China is often blamed for high-level cyber-espionage,bothpoliticalandeconomic.However,thereislittlehard evidenceforthis.
- As there is noway to clearly identifyperpetrators thatwanttostayhiddenincyberspace(attributionprob-lem), anyone could be behind actions that seeminglybenefitcertainstates.Statescanalsoplausiblydenybeinginvolved.
- Politicallymotivatedoractivistbreak-insbyhackercollec-tivesthatgoafterhigh-leveltargets,withtheaimtostealand publish sensitive information or just ridiculing themby targeting their websites, have recently added to thefeelingofinsecurityingovernmentcircles.

Table27.2Cyber-crimeandcyber-espionage

Name of incident	Yearof occurrence	Description	Perpetrators
414sbreak-ins	1982	Break-insintohigh-profilecomputersystemsintheUnited States	Sixteenage hackers from Milwaukee
HanoverHackers (Cuckoo'sEgg)	1986–1988	Break-insintohigh-profilecomputersystemsintheUnited States	Germanhackerrecruitedby theKGB
RomeLabincident	1994	Break-insintohigh-profilecomputersystemsintheUnited States	Britishteenagehackers
Citibankincident	1994	$10millionsiphonedfromCitibankandtransferredthe moneytobankaccountsaroundtheworld	Russianhacker(s)
SolarSunrise	1998	SeriesofattacksonDoDcomputernetworks	Twoteenagehackersfrom CaliforniaplusoneIsraeli
MoonlightMaze	1998	Patternofprobingofhigh-profilecomputersystems	AttributedtoRussia
TitanRain	2003–	Accesstohigh-profilecomputersystemsintheUnited States	AttributedtoChina
ZeusBotnet	2007	Trojanhorse'Zeus',controlledmillionsofmachinesin 196countries	Internationalcyber-crime network,over90people arrestedinUSalone
GhostNet	2009	Cyber-spyingoperation,infiltrationofhigh-valuepolitical, economic, andmedialocations in103countries	AttributedtoChina
OperationAurora	2009	Attacks against Google and other companies togain access toandpotentiallymodifysourcecoderepositoriesatthese hightech,security,anddefencecontractorcompanies	AttributedtoChina
WikileaksCablegate	2010	251,287leakedconfidentialdiplomaticcablesfrom274US embassiesaroundtheworld,datedfrom28December 1966to28February2010	Wikileaks,not-for-profit activistorganization
OperationsPayback andAvengeAssange	2010	Coordinated,decentralizedattacksonopponentsof Internetpiracyandcompanieswithperceivedanti-WikiLeaksbehaviour	Anonymous,hackercollective
Sonyandother corporateaswellas governmentattacks	2011	Highlypublicizedhacktivistoperations	LulzSec,hackercollective
TheftofCO2-EmmissionPapers	2011	Theftof475,000carbondioxideemissionsallowances worth€6.9million,or$9.3million	Attributedtoorganized cyber-crime(purpose probablymoneylaundering)
NSArevelations	2013	Leakingofclassifiedinformationthatshowedtheextent of(USgovernment)surveillanceprogramsthrough cyber-means	UnitedStatesNational SecurityAgency(NSA)
SonyPicturesHack	2014	SeriesofhacksanddatareleaseaboutSonyinternational, cumulatingincancellationofmovie'TheInterview'(which showsviolentdeathofNorthKoreanleaderKimJongUn)	AttributedtoNorthKorea (doubtful)

Cyber(ed)conflictsandvitalsystemsecurity (military–civil defencediscourse)

TheGulfWarof1991createdawatershedinUSmili-tary thinking about cyber-war. Military strategists sawtheconflictasthefirstofanewgenerationof**informa-tionage**conflictsinwhichphysicalforcealonewasnotsufficient,butwascomplementedbytheabilitytowinthe information war and to secure ‘information domi-nance’. As a result, American military thinkers beganto publish scores of books on the topic and developeddoctrines that emphasized the ability to degrade oreven paralyse an opponent’s communications systems(cf.Campen1992;ArquillaandRonfeldt1993).

Inthemid-1990s,theadvantagesoftheuseanddis-semination of ICT that had fuelled the revolution inmilitaryaffairswerenolongerseenonlyasagreatop-portunityprovidingthecountrywithan‘informationedge’(NyeandOwens1996),butwerealsoperceivedasconstitutinganover-proportionalvulnerabilityvis-à-visaplethoraofmaliciousactors.GlobalinformationnetworksseemedtomakeitmucheasiertoattacktheUSasymmetricallyand,assuch,anattacknolongerrequiredbig,specializedweaponssystemsoranarmy:borders,alreadyporousinmanywaysintherealworld,werenon-existentincyberspace.TherewaswidespreadfearthatthoselikelytofailagainsttheAmericanmili-tarywouldinsteadplantobringtheUSAtoitskneesbystrikingvitalpointsfundamentaltothenationalse-curity and the essential functioning of industrializedsocietiesathome.Apartfrombreak-insintocomputernetworksthatcontainedsensitiveinformation(seepre-vioussection),exercisesdesignedtoassesstheplausibil-ityofinformationwarfarescenariosandtohelpdefinekeyissuestobeaddressedinthisareademonstratedthat

US critical infrastructure presented a set of attractivestrategictargetsforopponentspossessinginformationwarfarecapabilities,beitterroristgroupsorstates.

Atthesametime,thedevelopmentofmilitarydoc-trineinvolvingtheinformationdomaincontinued.Forawhile,**informationwarfare**remainedessentiallylim-itedtomilitarymeasuresintimesofcrisisorwar.Thisbegantochangearoundthemid-1990s,whentheactivi-tiesbegantobeunderstoodasactionstargetingtheentireinformation infrastructure of an adversary—political,economic,andmilitary,throughoutthecontinuumofoperations from peace to war. NATO’s 1999 interven-tionagainstYugoslaviamarkedthefirstsustaineduseofthefull-spectrumofinformationwarfarecomponentsincombat.Muchofthisinvolvedtheuseofpropagandaand disinformation via the media (an important aspectof information warfare), but there were also websitedefacements,anumberofDDoS-attacks,and(unsub-stantiated)rumoursthatSlobodanMilosevic’sbankac-countshadbeenhackedbytheUSarmedforces.

TheincreasinguseoftheInternetduringthecon-flictgaveitthedistinctionofbeingthe‘firstwarfoughtincyberspace’orthe‘firstwarontheInternet’.There-after, the term cyber-war came to be widely used torefertobasicallyanyphenomenoninvolvingadelib-eratedisruptiveordestructiveuseofcomputers.Forexample, the cyber-confrontations between Chineseand US hackers plus many other nationalities in 2001havebeenlabelledthe‘firstCyberWorldWar’.Thecause was a US reconnaissance and surveillance planethatwasforcedtolandonChineseterritoryafteracolli-sionwithaChinesejetfighter.In2007,DDoS-attacksonEstonianwebsiteswerereadilyattributedtotheRussiangovernment,andvariousgovernmentofficialsclaimedthatthiswasthefirstknowncaseofonestatetarget-inganotherusingcyber-warfare(seeCaseStudy27.1).

CASESTUDY27.1Estonian‘cyber-war’

WhentheEstonianauthoritiesremovedabronzestatueofa SecondWorldWar-eraSovietsoldierfromaparkacyberspace-‘battle’ensued,lastingoverthreeweeks,inwhichawaveofso-

DistributedDenialofServiceattacks(DDoS)swamped variouswebsites—amongthemthewebsitesoftheEstonian parliament,banks,ministries,newspapers,andbroadcasters—

g thembyovercrowdingthebandwidthsfortheservers

sites.

readilyandpubliclyblamedtheRussiangovernment.Also, despitethefactthattheattacksborenotrulyserious

consequencesforEstoniaotherthan(minor)economiclosses,called some officials even openly toyed with the idea of a counter-attackinthespiritofArticle5oftheNorthAtlanticTreaty,

whichstatesthat‘anarmedattack’againstoneormoreNATOdisablin

countries‘shallbeconsideredanattackagainstthemall’.Therunningthe Estoniancaseisoneofthecasesmostoftenreferredtoin

Similar claims were made in the confrontation be-tween Russia and Georgia of 2008. In other cases,Chinaissaidtobetheculprit(seeprevioussectionandTable27.3).
The discovery ofStuxnet in 2010 changed theoverall tone and intensity of the debate (see CaseStudy27.2).

Table27.3Instances ofcyber(ed)-conflict

Name of incident	Yearofoccurrence	Description	Actors/perpetrators
GulfWar	1991	Firstof a new generationof conflicts where victoryisnolongerdependentonlyon physicalforce,butalsoontheabilitytowinthe informationwarandtosecure'information dominance'	US military
Dutch hacker incident	1991	IntrusionsintoPentagoncomputersduringGulf War.Accesstounclassified,sensitiveinformation	Dutchteenagers
Operation'AlliedForce'	1999	'ThefirstInternetWar':sustaineduseofthefull-spectrumofinformationwarfarecomponentsin combat.Numeroushacktivismincidents	USmilitary,hacktivistsfrom manycountries
'Cyber-Intifada'	2000–2005	E-mailfloodingandDenial-of-Service(DoS) attacksagainstgovernmentandpartisan websitesduringsecondIntifada	PalestinianandIsraeli hacktivists
'CyberWorld-WarI'	2001	DefacementofChineseandUSwebsitesand wavesofDDoS-attacksafterUSreconnaissance andsurveillanceplanewasforcedtolandon Chineseterritory	Hacktivists from manynations (SaudiArabia,Pakistan,India, Brazil,Argentina,Malaysia, Korea,Indonesia,Japan)
Iraq	2007	Cyber-attackoncellphones,computers,and othercommunicationdevicesthatterrorists wereusingto planand carryoutroadside bombs	US military
EstoniaDDoS-attacks	2007	DDoS-attacksagainstwebsitesoftheEstonian parliament,banks,ministries,newspapers,and broadcasters	AttributedtoRussian government
GeorgiaDDoS-attacks	2008	DDoS-attacksagainstnumerousGeorgian websites	AttributedtoRussian government
GhostNetinfiltrations	2009	GhostNetrelatedinfiltrationsofcomputers belonging toTibetan exilegroups	AttributedtoChinese government
Stuxnet	2010	Computerwormthatmighthavebeen deliberatelyreleasedtoslowdownIranian nuclearprogramme	USgovernment(+Israel)
Koreannetwork intrusions	2011	BotnetsandDDos-attacksagainstgovernment websites.ExpertssuspectedNorthKorean 'cyber-weapons'test	AttributedtoNorth-Korean government

Due to the attribution problem, it was impossi-bletoknowforcertainwhowasbehindthispieceofcode,thoughmanysuspectedoneorseveralstateac-tors(FarwellandRohozinski2011).InJune2012,aninvestigativejournalistsuggestedthatStuxnetispartof a US and Israeli intelligence operation and that itwasindeedprogrammedandreleasedtosabotagethe

CASESTUDY27.2Stuxnet

Stuxnetisacomputerwormthatwasdiscoveredin June2010and hasbeencalled'[O]neofthegreattechnicalblockbustersin malwarehistory'(Gross2011).Itisacomplexprogram.Itislikely werebehindthatwritingittookasubstantialamountoftime,advanced-level theprogrammingskillsandinsiderknowledgeofindustrialprocesses. Therefore,Stuxnetwasthemostexpensivemalwareeverfoundat thattime.Inaddition,itbehavesdifferentlyfrommalwarereleased forcriminalintent:itdoesnotstealinformationanditdoesnot first, herdinfectedcomputersintoso-calledbotnetsfromwhichto launchfurtherattacks.Rather,itlooksforaveryspecifictarget: StuxnetwaswrittentoattackSiemens'*SupervisoryControlAndData Acquisition*(SCADA)systemsthatareusedtocontrolandmonitor be increasinglyindustrialprocesses.InAugust2010,thesecuritycompany Symantecnotedthat60percentoftheinfectedcomputers undertaken.worldwidewereinIran.ItwasalsoreportedthatStuxnetdamaged

centrifugesintheIrannuclearprogramme.Thisevidenceled severalexpertstotheconclusionthatoneorseveralnation states—mostoftennamedaretheUSAand/orIsrael- the attack. No official statement has ever been issued, but involvementoftheUSgovernmentseemsquitecertainbynow.

Onanothernote,Stuxnetprovidedaplatformforanever-growing host of cyber-war-experts to speculate about the future of cyber-aggression. Internationally, Stuxnethas had two main effects: governmentsalloverthe worldarecurrentlyreleasingorupdating cyber-securitystrategiesandaresettingupneworganizational units for cyber-defence (and -offence). Second, Stuxnet can considered a 'wake-up' call: ever since its discovery, seriousattemptstocometosometypeofagreementonthenon-aggressive use of cyberspace between states are

Iraniannuclearprogramme.Formanyobservers,Stux-net as a 'digital first strike' marks the beginning of theunchecked use of **cyber-weapons** in military-like ag-gressions(Gross2011).However,otherreportsthinkthisunlikely(cf.SommerandBrown2011),mainlyduetotheuncertainr esultsacyber-warwouldbring,thelack of motivation on the part of the possible com-batants, and their shared inability to defend againstcounterattacks.

Future conflicts between nations will most cer-tainlyhaveacyberspacecomponentbuttheywillbejustapartofthebattle.Itisthereforemoresensible to speak about cyber(ed) conflicts, conflicts 'in whichsuccessorfailureformajorparticipantsiscriticallyde-pendent on computerized key activities along the pathof events' (Demchak2010). Dubbing occurrences as'cyber-war' too carelessly bears the inherent dangerof creating an atmosphere of insecurity and tensionandfuellingacyber-securitydilemma:manycountriesare currently said to have functional cyber-commandsorbeintheprocessofbuildingone.Becausecyber-capabilities cannot be divulged by normal intelligencegathering activities, uncertainty and mistrust are ontherise.

KEYPOINTS

- TheGulfWarof1991isconsideredtobethefirstofanew generationofconflictsinwhichmasteringtheinformation domainbecomesadecidingfactor.Afterwards,theinforma-tionwarfaredoctrinewasdevelopedintheUSmilitary.
- Increasingdependenceofthemilitary,butalsoofsociety ingeneral,oninformationinfrastructuresmadeclearthat informationwarfarewasadouble-edgedsword.Cyberspace seemedtheperfectplacetolaunchanasymmetricalattack againstcivilianormilitarycriticalinfrastructures.
- TheUSmilitarytesteditsinformationwarfaredoctrine forthefirsttimeduringaNATOoperation'AlliedForce' in1999.Itwasthefirstarmedconflictinwhichallsides, includingactorsnotdirectlyinvolved,hadanactiveonline presence,andinwhichtheInternetwasactivelyusedforthe exchangeandpublicationofconflict-relevantinformation. Thereafter,theterm'cyber-war'cametobeusedforalmost anytype ofconflict witha cyber-component.
- Therecentdiscoveryofacomputerwormthatsabotages industrialprocessesandwasprogrammedbyorderofa stateactorhasalarmedtheinternationalcommunity.Some expertsbelievethatthismarksthebeginningofunre-strainedcyber-war amongstates.
- Othersthinkthathighlyunlikelyandwarnagainstanexces-siveuse of theterm cyber-war. Future conflictsbetween stateswillalsobefoughtincyberspace,butnotexclusively. Oneusefultermforthemiscyber(ed)conflicts.

KEYIDEAS27.1PresidentialCommissiononCriticalInfrastructureProtection

FollowingtheOklahomaCityBombing,PresidentBillClinton
whicharesusceptibletoclassicalphysicaldisruptionsandnewsetupt
hePresidentialCommissiononCriticalInfrastructure
virtualthreats.While thestudyassesseda
listofcriticalProtection(PCCIP)tolookintothesecurityofvitalsystems infrastructuresor'sectors'—forexamplethefinancialsector,
suchasgas,oil,transportation,water,telecommunications,
energysupply,transportation,andtheemergencyservices—
etc.ThePCCIPpresenteditsreportinthefallof1997
themainfocuswasoncyber-
risks.Thereweretworeasons(PresidentialCommissiononCriticalInfrastructureProtection
forthisdecision:first,thesewerethe leastknownbecause1997).
Itconcluded thatthesecurity, economy,way oflife,and
theywerebasicallynew,andsecond,manyoftheotherperhapsevent
hesurvivaloftheindustrializedworldwere
infrastructureswereseentodependondataand
dependentontheinterrelatedtrioofelectricalenergy,
communication networks. The PCCIP linked the cyber-

Reducingcyber-in-security

The three different discourses have produced specifictypes of concepts and countermeasures in accord-ance with their focus and main referent objects (seeFigure27.2),someofwhicharediscussedlater.

Despite fancy concepts such as **cyber-deterrence**,the common issue in all discourses is information as-surance, which is the basic security of informationandinformationsystems.Itiscommonpracticethattheentitiesthatownacomputernetworkarealsore-sponsibleforprotectingit(governmentsprotectgov-ernmentnetworks,militariesonlymilitaryones,andcompanies protect their own, etc.). However, thereare some assets considered so crucial to the function-ingofsocietyintheprivatesectorthatgovernmentstakeadditionalmeasurestoensureanadequatelevelof protection. These efforts are usually subsumedunder the label of **critical (information) infrastruc-tureprotection**.

In the 1990s, critical infrastructures became themain referent object in the cyber-security debate.Whereas critical infrastructure protection (CIP) en-compassesmorethanjustcyber-security,cyber-aspectshavealwaysbeenthemaindriver(seeKeyIdeas27.1).ThekeychallengeforCIPeffortsarisefromthepri-vatization and deregulation oflarge parts ofthepublic sector since the 1980s and the globalizationprocessesofthe1990s,whichhaveputmanycriticalinfrastructuresinthehandsofprivate(transnational)enterprises.Thiscreatesasituationinwhichmarketforcesalonearenotsufficienttoprovidetheaspiredforlevelofsecurityindesignatedcriticalinfrastructure
sectors,1 but state actors are also incapable of pro-viding the necessary level of security on their own(unlesstheyheavilyregulate,whichtheyareusuallyreluctanttodo).

Public–Private Partnerships (PPP), a form of co-operation between the state and the private sector,are widely seen as a panacea for this problem in the**policy community**—and cooperation programmesthat follow the PPP idea are part of all existing initia-tives in the field of CIP today, though with varyingsuccess.Alargenumberofthemaregearedtowardsfacilitating information exchange between companiesandbetweencompaniesandgovernmentonsecurity,disruptions, and best practices. Mutual win–win situ-ations are to be created by exchanging informationthattheotherpartydoesnothave:thegovernmentof-fers classified information acquired by its intelligenceservices about potentially hostile groups and nationstates in exchange for technological knowledge fromtheprivatesectorthatthepublicsectordoesnothave(President's Commission on Critical InfrastructureProtection1997:20).

Information assurance is guided by the manage-ment of risk, which is essentially about accepting thatoneis(orremains)insecure:thelevelofriskcanneverbereducedtozero.Thismeansthatminorandprob-ablyalsomajorcyber-incidentsareboundtohappen

1Themostfrequentlylistedexamplesarebankingandfi-nance,governmentservices,telecommunicationandinfor-mation and communication technologies, emergency andrescueservices,energyandelectricity,healthservices,trans-portation,logisticsanddistribution,andwatersupply.

Figure27.2Countermeasures

	Technical	**Crime–Espionage**	**Military/civildefence**
Mainactors	▪ Computerexperts ▪ Anti-virusindustry	▪ Lawenforcement ▪ Intelligencecommunity	▪ Security professionals,military,civildefenceestablishment
Mainreferentobject	▪ Computers ▪ Computernetworks	▪ Businesssector ▪ Classifiedinformation	▪ Military networks,networkedforces ▪ Criticalinfrastructures
Protection concept	Informationassurance		
National level	▪ CERTs(specificfor differentdomain, milCert,govCertetc.)	▪ Computerlaw	▪ Critical (information)infrastructureprotection ▪ Resilience ▪ Cyber-offence;cyber-defence; cyber-deterrence
International level	▪ InternationalCERTs ▪ Internationalinformationsecuritystandards	▪ Harmonization oflaw (Convention onCybercrime) ▪ Mutualjudicialassistanceprocedures	▪ Armscontrol ▪ Internationalbehaviouralnorms

because they simply cannot be avoided even with per-fect risk management. This is one of the main reasonswhy the concept of resilience has gained so muchweight in recent debates (Perelman 2007). Resilienceiscommonlydefinedastheabilityofasystemtore-cover from a shock, either returning back to its origi-nal state or to a new adjusted state. Resilience acceptsthatdisruptionsareinevitableandcanbeconsidereda‘PlanB’incasesomethinggoeswrong.

Inthemilitarydiscourse,thetermscyber-offence,cyber-defence, and cyber-deterrence are often usedas countermeasures. Under closer scrutiny, cyber-de-fence(andtosomedegree-offence)arenotmuchmorethan fancy words for information assurance practices.Cyber-deterrence on the other hand deserves some at-tention. Cyberspace clearly poses considerable limita-tions for classical deterrence. Deterrence works if onepartyisabletosuccessfullyconveytoanotherthatitisbothcapableandwillingtouseasetofavailable(often military) instruments against him if the other stepsover the line. This requires an opponent that is clearlyidentifiable as an attacker and has to fear retaliation—which is not the case in cyber-security because of theattribution problem. However, this is not stopping USgovernmentofficialsfromthreateningtousekineticresponseincaseofacyber-attackontheircriticalin-frastructures(GormanandBarnes2011).

Naturally, the military discourse falls back on well-known concepts such as deterrence, which means thattheconceptofcyber-deterrence,includingitslimits,will remain a much discussed issue in the future. Intheory, effective cyber-deterrence would require awide-rangingschemeofoffensiveanddefensivecyber-capabilitiessupportedbyarobustinternationallegalframeworkaswellastheabilitytoattributeanattackto an attacker without any doubt. The design of de-fensivecyber-capabilitiesandthedesignofbetterlegaltools are relatively uncontested. Many internationalorganizations and international bodies have takenstepstoraiseawareness,establishinternationalpart-nerships, and agree on common rules and practices.One key issue is the harmonization of law to facilitatetheprosecutionofperpetratorsofcyber-crime.

While there is wide agreement on what steps arenecessary to tackle international cyber-crime, statesare unwilling to completely forgo offensive and ag-gressiveuseofcyberspace.Duetothis,andincreas-ingly so since the discovery of Stuxnet, efforts areunderway to control the military use of computerexploitationthrougharmscontrolormultilateral

behavioural**norms**, agreements that might pertaintothedevelopment,distribution,anddeploymentofcyber-weapons,ortotheiruse.However,traditionalcapability-based arms control will clearly not be ofmuchuse,mainlyduetotheimpossibilityofverify-ing limitations on the technical capabilities of actors,especially non-state ones. The avenues available forarms control in this arena are primarily informationexchangeandnorm-building,whereasstructuralapproaches and attempts to prohibit the means ofcyber-war altogether or restricting their availabilityare largely impossible due to the ubiquity and dual-usenatureofinformationtechnology.

KEYPOINTS

- Thereareavarietyofapproachesandconceptstosecureinformation and critical information infrastructures. Thekey concept is a risk management practice known asinformation assurance, which aimsto protect theconfi-dentiality,integrity,andavailabilityofinformationandthesystemsandprocessesusedforthestorage,processing,andtransmissionofinfor mation.
- Critical(information)infrastructureprotection(C(I)IP)hasbecome a key concept in the 1990s. Because a very largepart of critical infrastructuresare no longerin the handsof government, CIP practices mainly build on public-pri-vate partnerships. At the core of them lies informationsharingbetweentheprivateandthepublicsector.
- Because the information infrastructure is persuasivelyinsecure,riskmanagementstrategiesarecomplementedby the concept of resilience. Resilience is about havingsystemsreboundfromshocksinanoptimalway.Thecon-cept accepts that absolute security cannot be obtainedandthatminororevenmajordisturbancesareboundtohappen.
- Themilitaryconceptsofcyber-defenceandcyber-offenceare militarized words for information assurance practices.Cyber-deterrence,ontheotherhand,isaconceptthatmovesdeterrenceintothenewdomainofcyberspace.
- Ifcyber-deterrenceweretowork,functioningoffensiveanddefensivecyber-capabilities,plusthefearofretali-ation,bothmilitarilyandlegally,wouldbeneeded.Thiswouldalsoincludetheabilitytoclearlyattributeattacks.
- Internationally, efforts are underway to further harmonizecyber-law. In addition, because future use of cyberspaceforstrategicmilitarypurposesremainsoneofthebiggestfearsinthedebate,thereareattemptstocurtailthemili-taryuseofcomputerexploitationthrougharmscontrolormultilateralbehaviouralnorms.

Thelevelofcyber-risk

Different political, economic, and military conflictsclearly have had cyber(ed)-components for a numberof years now. Furthermore, criminal and espionageactivities with the help of computers happen everyday. Cyber-incidents are causing minor and occasion-allymajorinconveniences.Thesemaybeintheformof lost intellectual property or other proprietary data,maintenance and repair, lost revenue, and increasedsecuritycosts.Beyondthedirectimpact,badlyhan-dled cyber-attacks have also damaged corporate (andgovernment) reputations and have, theoretically atleast,thepotentialtoreducepublicconfidenceinthesecurity of Internet transactions and e-commerce iftheybecomemorefrequent.

However, in the entire history of computer net-works, there have been only very few examples ofattacksorothertypeofincidentsthathadthepoten-tialtorattleanentirenationorcauseaglobalshock.Thereareevenfewerexamplesofcyber-attacksthatresulted in actual physical violence against persons orproperty (Stuxnet being the most prominent). Thehugemajorityofcyber-incidentshavecausedminorlosses rather than serious or long-term disruptions.Theyarerisksthatcanbedealtwithbyindividualenti-ties using standard information security measures andtheiroverallcostsremainlowincomparisontootherriskcategorieslikefinancialrisks.

Thisfacttendstobedisregardedinpolicycircles,becausethelevelofcyber-fearsishighandthemilitarydiscourse has a strong mobilizing power. This has im-portantpoliticaleffects.Alargepartofthediscourseevolvesaround‘cyber-doom’(worst-case)scenariosinthe form of major, systemic, catastrophic incidents in-volvingcriticalinfrastructurescausedbyattacks.Sincethe potentially devastating effects of cyber-attacks areso scary, the temptation to not only think about worst-case scenarios but also give them a lot of (often toomuch) weight despite their very low probability ishigh.

There are additional reasons why the threat is over-rated. First, as combating cyber-threats has become ahighly politicized issue, official statements about thelevel of threat must also be seen in the context ofdifferent bureaucratic entities that compete againsteach other for resources and influence. This is usu-ally done by stating an urgent need for action (whichthey should take) and describing the overall threatasbigandrising.Second,psychologicalresearchhas

shown that risk perception is highly dependent onintuitionandemotions,aswellastheperceptionsof experts (Gregory and Mendelsohn 1993). Cyber-risks, especially in their more extreme form, fit therisk profile of so-called ‘dread risks’, which appearuncontrollable,catastrophic,fatal,andunknown.There is a propensity to be disproportionally afraidof these risks despite their low probability, whichtranslates into pressure for regulatory action of allsorts and a willingness to bear high costs of uncer-tainbenefit.

The danger ofoverly dramatizing the threat man-ifests itselfin reactions that call for military retalia-tion (as happened in the Estonian case and in otherinstances) or other exceptional measures. Thoughthe last section has shown that there are many dif-ferent types of countermeasures in place, and thatmost ofthem are in fact not exceptional, this kindofthreat rhetoric invokes enemy images even ifthere is no identifiable enemy, favours national so-lutions instead ofinternational ones, and centrestoo strongly on national-security measures insteadofeconomic and business solutions. Only computerattackswhoseeffectsaresufficientlydestructiveor disruptive need the attention ofthe traditionalnationalsecurityapparatus.Attacksthatdisruptnon-essential services, or that are mainly a costlynuisance,shouldnot.

KEYPOINTS

- Themajorityofcyber-incidentssofarhavecausedminorinconveniencesandtheircostremainslowincomparisonto other risk categories. Only very few attacks had thepotential for grave consequences and even fewer actuallyhadanyimpactonproperty.Nonehaveevercausedlossoflife.
- Despitethis,thefeelingpersistsinpolicycirclesthatalarge-scale cyber-attack is just around the corner. Thepotentialforcatastrophiccyber-attacksagainstcriticalinfrastructures, though very unlikely, remains the mainconcernandthemainreasonforseeingcyber-securityasanationalsecurityissue.
- The level of cyber-risk is overstated. Reasons are to befoundinbureaucraticturfbattlesduetoscarceresourcesandinthefactthatcyber-risksaresocalled‘dreadrisks’,of which human beings are disproportionally afraid.Overstatingtheriskcomeswiththedangerofprioritizingthewronganswers.

CONCLUSION

Despite the increasing attention cyber-security is get-tinginsecuritypoliticsanddespitethepossibilityofa major, systemic, catastrophic incident involvingcritical infrastructures, computer network vulner-abilities are mainly a business and espionage problem.Depending on their (potential) severity, however, dis-ruptive incidents in the future will continue to fuelthe military discourse, and with it fears of strategiccyber-war. Certainly, thinking about (and planningfor)worst-casescenariosisalegitimatetaskofthena-tional security apparatus. However, they should notreceive too much attention in favour of more plausibleandmorelikelyproblems.

In seeking a prudent policy, the difficulty for deci-sionmakersistonavigatetherockyshoalsbetweenhysterical doomsday scenarios and uninformed com-placency.Threat-representationmustremainwellin-formed and well balanced not to allow over-reactionswithcoststhataretoohighandbenefitsthatareuncer-tain. For example, an 'arms race' in cyberspace, basedonthefearofotherstates'cyber-capabilities,wouldmost likely have hugely detrimental effects on theway humankind uses the Internet. Also, solving theattribution problem would come at a very high costfor privacy. Even though we must expect disturbancesinthecyber-domaininthefuturewemustnotexpectoutrightdisasters.Someofthecyber-disturbances may well turn into crises, but a crisis can also be seenas a turning point rather than an end state where theaversion of disaster or catastrophe is always possible.If societies become more fault tolerant psychologi-cally and more resilient overall, the likelihood for ca-tastrophe in general and catastrophic system failure inparticularcanbesubstantiallyreduced.

Cyber-securityissuesarealsochallengingforstu-dents and academics more generally. Experts of allsorts widely disagree how likely future cyber-doomscenarios are—and all of their claims are based on(educated)guesses.Whilethereisatleastproofandexperience of cyber-crime, cyber-espionage, or otherlesser forms of cyber-incidents on a daily basis, cy-ber-incidents ofbigger proportions (**cyber-terror** orcyber-war)existsolelyintheformofstoriesornar-ratives. The way we imagine them influences ourjudgement of their likelihood; and there are an infi-nitenumberofwaysinhowwecouldimaginethem.Therefore,thereisnowaytostudythe'actual'levelofcyber-riskinanysoundwaybecauseitonlyexistsinand through the representations of various actors inthepoliticaldomain.Asaconsequence,thefocusofresearchnecessarilyshiftstocontextsandconditionsthatdeterminetheprocessbywhichkeyactorssubjec-tively arrive at a shared understanding of how to con-ceptualizeandultimatelyrespondtoasecuritythreat.