

PROF. DR. JUAN CARLOS BARRERA

CYBER-SECURITY (BC6)

July 2020

Online Germany

Broadcasting from USA







Ecosystems of the Cyberspace

DAY 05

Agenda:

1) Cyber-Innovations: Deep Web + + +

2) Videos: Discussion & Reflection

3) Fifth Lab

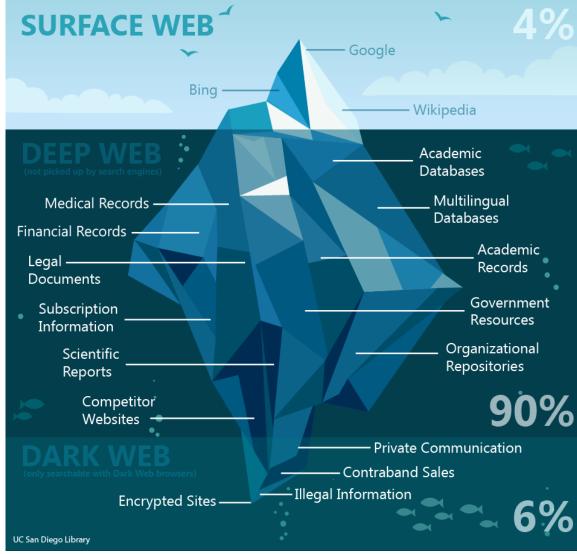
4) Economics of Cybersecurity

5) In Closing: Debriefing for Cases 01 - 02 - 03 - 04

1) Cyber-Innovations: Deep Web +

1) Deep Web Fundamentals

The deep Web, sometimes called the invisible Web, is the large part of the Internet that is inaccessible to conventional search engines. Deep Web content includes email messages, chat messages, private content on social media sites, electronic bank statements, electronic health records (EHRs) and other content that is accessible over the Internet but is not crawled and indexed by search engines like Google, Yahoo, Bing or DuckDuckGo.



Surface Web

- The surface Web is that portion of the World Wide Web that is indexable by conventional search engines.
- It is also known as the Clearnet, the visible Web or indexable Web.
 - Eighty-five percent of Web users use search engines to find needed information, but nearly as high a percentage cite the inability to find desired information as one of their biggest frustrations.
- A traditional search engine sees only a small amount of the information that's available -- a measly 0.03 % [source: OEDB].



- Jill Ellsworth used the term invisible Web in 1994 to refer to websites that were not registered with any search engine.
- Mike Bergman cited a January 1996 article by Frank Garcia:

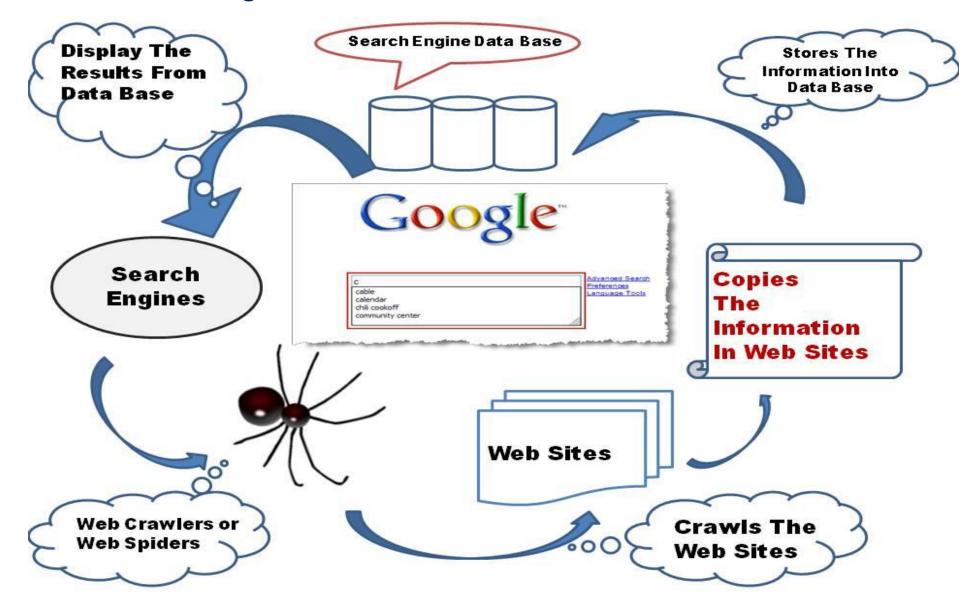
"It would be a site that's possibly reasonably designed, but they didn't bother to register it with any of the search engines. So, no one can find them! You're hidden. I call that the invisible Web".

- Another early use of the term Invisible Web was by Bruce Mount and Matthew B.
 Koll of Personal Library Software in 1996.
- The first use of the specific term Deep Web, now generally accepted, occurred in the aforementioned 2001 Bergman study.

How search engines work

- Search engines construct a database of the Web by using programs called spiders or Web crawlers that begin with a list of known Web pages.
- The spider gets a copy of each page and indexes it, storing useful information that will let the page be quickly retrieved again later.
- Any hyperlinks to new pages are added to the list of pages to be crawled.
- Eventually all reachable pages are indexed, unless the spider runs out of time or disk space.
- The collection of reachable pages defines the Surface Web.

How search engines work



Contents

Dynamic content:

- Dynamic pages which are returned in response to a submitted query or accessed only through a form
- Especially if open-domain input elements (such as text fields) are used
- Such fields are hard to navigate without domain knowledge

Unlinked Content:

- Pages which are not linked to by other pages
- Which may prevent web crawling programs from accessing the content
- This content is referred to as pages without backlinks (or in links).

Contents (cont'd)

Private Web:

- Sites that require registration and login (password-protected resources).
 Contextual Web:
- Pages with content varying for different access contexts (e.g., ranges of client IP addresses or previous navigation sequence).

Limited access content:

 Sites that limit access to their pages in a technical way (e.g., using the Robots Exclusion Standard, CAPTCHAs, or no-cache Pragma HTTP headers which prohibit search engines from browsing them and creating cached copies.

Contents (cont'd)

Scripted content:

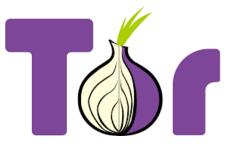
 pages that are only accessible through links produced by JavaScript as well as content dynamically downloaded from Web servers via Flash or Ajax solutions.

Non-HTML/text content:

 textual content encoded in multimedia (image or video) files or specific file formats not handled by search engines.

Access to the Deep Web

Tor



The Tor software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked." – www.torproject.org

 Tor is a network that supports onion routing; a way to help make your traffic anonymous. Because the Deep Web is compromised of information that doesn't show up on search engines, or has no domain name registry, you must know exactly where you are going to get there.

Access (cont'd)

- Tor is software that installs into your browser and sets up the specific connections you need to access dark Web sites.
- Critically it is free software for enabling online anonymity and censorship resistance.
- Onion routing refers to the process of removing encryption layers from Internet communications, similar to peeling back the layers of an onion.
- Using Tor makes it more difficult to trace Internet activity, including "visits to Web sites, online posts, instant messages, and other communication forms", back to the user.
- It is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential business by keeping their internet activities from being monitored.

Access (cont'd)

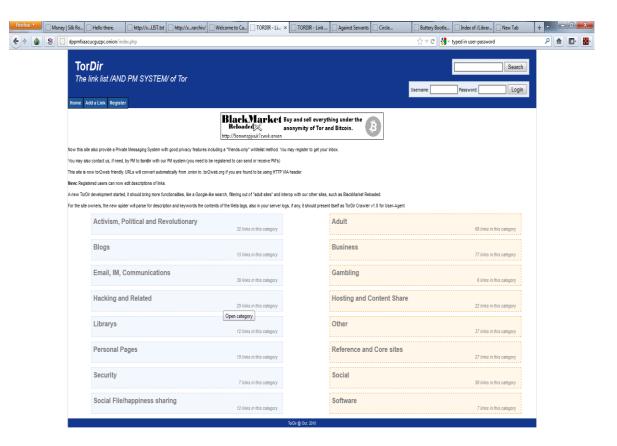
- Instead of seeing domains that end in .com or .org, these hidden sites end in .onion.
- The most infamous of these onion sites was the now-defunct Silk Road, an online marketplace where users could buy drugs, guns and all sorts of other illegal items.
- The FBI eventually captured Ross Ulbricht, who operated Silk Road, but copycat sites like Black Market Reloaded are still readily available.
- Tor is the result of research done by the U.S. Naval Research Laboratory, which created Tor for political dissidents and whistleblowers, allowing them to communicate without fear of reprisal.
- Tor was so effective in providing anonymity for these groups that it didn't take long for the criminally-minded to start using it as well.

Inside the Deep Web

• The next step is to access the Hidden Wiki, which most people consider the home page of the Deep Web. Here you can begin your journey and discover many different types of sites and networks, ranging from tame to very illegal. There are black market type sites, hacking information sites, huge file databases, political advocacy sites, and even sites to hire people to engage in illegal activity.

Firefox 🔹 🤇 🚺	Services Sil Hello there.	http://ST.txt Sea Kitten P	http:/rchiv/	Welcome to	TORDIR - Li	TORDIR - Li	🗍 TORDIR - Li	Against Ser	Circle	BlackMarke	🗌 - Guns - Ha	Buttery I 🕻	+ • 🖻	- Ó - X		
(-) 💧 😒	7jguhsfwruviatqe.onion/inc	dex.php/Main_Page							☆ ⊽ C	f 🚼 - typed in u	user-password		<mark>ا</mark>	D- 🛛		
	page discussion	view source history										1	Log in / crea	ite account		
The Hidden Wiki		,														
K	indiri rugo															
•	About this Wik	(i										Contents [hide]				
	News / History	News / History														
vigation Main page	· · ·												1.2 Comms 1.3 Editor's picks			
All pages	 Entries over 30 days old are moved to the Site News Archive. See this index for articles regarding anonymity, stenography, marketplaces, software, and other topics. 											1.4 Browsing / Mirroring				
Recent changes Random page													1.5 Volunteer TODO			
arch	Comms	Comms										2 Hidden services - HTTP/HTTPS 2.1 Introduction Points				
aui	ion@torpm - SiteOp - not checked very often											2.2 Tor Network				
Go Search	 OnionNet #hiddenwiki 											2.3 Marketplac				
uu Josiui		munity notepad for discussion, que			S.								ncial Service			
blbox	 Special:RecentChange 	es 🗗 - Discussion, questions, comp	plaints and sugges	stions									nmercial Serv Veb / File / Im			
What links here Related changes	Editor's picks											2.4 Hosting - Web / File / Image 2.4.1 Webhost comparison				
Special pages	Bored? Pick a random page from the article index and replace one of the five slots with it.											2.5 Blogs				
Printable version	1. TORCH @- Tor Search Engine. Claims to index around 600k pages.											2.6 Forums / Boards / Chans				
Permanent link	1. TORCH 2 - Tor Search Englie. Claims to index alound block pages. 2. List of Anonymous Networks - Try these out and learn from them.											2.7 Email / Messaging 2.8 Political Advocacy				
	3. Silk Road @ - Private marketplace with escrow. (Bitcoin)										2.9 Wikis					
	4. Needed Hidden Se	rvices - Ideas for hidden services to	benefit the Tor co	ommunity.								2.10 Whistleblowing				
	5. Eradic P - Quality Deepnet Supplier of Weed, LSD, and Ecstasy (BTC/Dwolla/LR) (Host: FH)											2.10.1 WikiLeaks 2.10.2 Operation AntiSec				
	Browsing / Mirroring															
		•										2.10.3 Other 2.11 HP/AWW/C 2.11.1 Phishing Sites				
	These links may be used	to browse or mirror all the pages in	this wiki:													
	» Special:AllPages @, Admin Dumps @, The Hidden Wik:Back up											2.12 Audio - Music / Streams				
	Volunteer TODO											2.13 Video - Movies / TV				
													 2.14 Books 2.15 Drugs 			
	Bored? Here are five random things to help out with.											2.15 Drugs 2.15.1 Noncommercial (D)				
	1. Plunder other hidden senice lists for links and place them here.										2.15.2 Commercial (D)					
	2. File the SnapBBSIndex links wherever they go. 3. Set extremel links to LITTIC where and extiliants, and extreme content										2.16 Erotica					
	Set external links to HTTPS where available, good certificate, and same content. Care to start recording onionland's history? Check out Onionland's Museum.											2.16.1 Above Age				
	Check the list of dead hidden services for services that have returned											2.16.1.1 Noncommercial (2.16.1.2 Commercial (E)				
												2.16.2 Un				
	Hidden servic	es - HTTP/HTTPS										2.17 Uncategorized				
	Volunteers last verified all	Volunteers last verified all senices in this section as up, or marked as DOWN, on: 2011-06-12											2.18 Non-English 2.18.1 Czech / Čeština			
	Introduction Points											2.18.2 Danish / Dansk				
	Chine and link indexes and search posinge											 2.18.3 Dutch / Nederlands 2.18.4 Finnish / Suomi 				
	OnionLand link indexes and search engines. TorMarks @ - The fastest-loadinn TOR directory around. (Host: FH)											2.18.5 French / Français				
	 IorMarks & - The faste 			1				1.0			100	6 M		5:09 PM		
🦻 (ê 🛭		🕐 💙 👛 🖞	8	In The	1000		1000	A Charles		140			N 🕽 🖗	4/4/2012		

One of the other "main pages" of the Deep Web is TorDir. TorDir is a site that uses a special crawler for the Deep Web, so that it may act similar to Google in that it categorizes web sites, and allows you to view many different and obscure .onion sites that fall into each category.



nfxaacucourne.onion/index.nhn?n=cat8/cid=48/sid=n0fcufnn01h7c9nokmnc9dn8

Through the Hidden Wiki you can find pages like this, which are semiorganized lists of different .onion sites. Many different sites are listed and separated based on function, such as buying/selling/trading, communication, hacking, or intel exchange.

efox 🔹	[] Money [ilk Ro 🗍 Hello the	nere. ht	:p://ST.txt ×	http://xrarchiv	/ 🗌 Welcome to Ca	🗍 TORDIR - Link	ORDIR - Link	Against Servants	Circle	Buttery Bootle	Index of /Librar	New Tab	+		
		xsin4xbme24aatvk.on									☆ ⊽ C 😽	 typed in user-passwor 	rd	٩)	•
		n - Buy Bitc					Junid Abordoni 10	1000.011011								
Hostin	ng file :	services: Ho:	sts files.													
Circle	eService	s - Most fam	ous place	in Onionl	and that pr	ovides all k	inds of serv	ices: http://	4eiruntyxxbqfv	70.onion/						
Onion	Filesha	re - 2GB upl	oad file s	ize limit	!!!: http:/	/f3ew3p7s6lb	ftqm5.onion/									
		lic file hos					iruntyxxpgiv	70.onion/past	.e/							
						hknwg4up2jhd	kx.onion/									
Hostin	ng websi	tes: Hosts .	onion webs	ites.												
									jieju2s4fc33.c							
		ng – Attacke ts forums: h					nion sites.	Currently, in	wite only: htt	p://xqz3u	5drneuzhaeo.on	ion/				
							elines for m	aking a site:	http://wf4df3	7hrebhwzts	s.onion/					
Chans,	/Imagebo	ards - Kind (of like 40	han and t	he likes. M	AY CONTAIN C	UESTIONABLE	CONTENT, none	right now the	ugh. USE V	WITH YOUR OWN	DISCRETION!!!				
Torcha	an - Sta	rted Decembe:	er 2011. Re	incarnati	on of Torch	an, the most	famous *cha	n to exist in	.onionland. U	sed to hav	ve heavy CP: h	ttp://zw3crggt	adila2sg.o	nion/ima	ageboa	rd/
Runda(Chan - S	tarted Decemi	uber 2011.	New chan.	Helpful to	newbies: ht	tp://vkfwagl	wnbi6vl7s.oni	.on/		-	1 33	-		-	
								za4fr.onion/i	mgboard/b/ sy5zg7aqze.oni	on/						
						awzy23.onion		iccp.//odoj4	ayszy/ayze.oni	011/						
Board	s: Mostl;	y SnapBBS. N	iormal foru	ms.												
Thieve	es Marke	t - Cheap pr:	ices, nice	goods: h	ttp://4eiru	ntyxxbqfv7o.	onion/snapbb	s/5595881d/								
									snapbbs/5112d4							
									nion/snapbbs/1 bbs/1b82f13e/	acda566/						
						3sce5.onion/		, o ronzon, onaj								
		ss anything:					. ,									
						2uzjw2wby3z. osl7r.onion/										
Netwo	rking: S	ocial networ	king.													
Torbo	ok – Fac	ebook for To:	or. Has a p					xtqy3fdlr.oni	on/torbook/							
Quest:	ions and	Answers - A	cool trut	h game: h	ttp://ajqai	vfxtqy3fdlr.	onion/qa/ind	ex.php								
Email,	/Messagi	ng: Communica	ation.													
		rivate messa														
Tor Ma	ail - Em	ail services	. *@tormai	l.net: ht	tp://jhiwjj	lqpyawmpjx.c	nion/									
Hax: H	Hacking,	etc.														
	artv - C	cacking site	: http://3	terbsb5mm	mdvhse.onio	n/										
							kjda7.onion/									

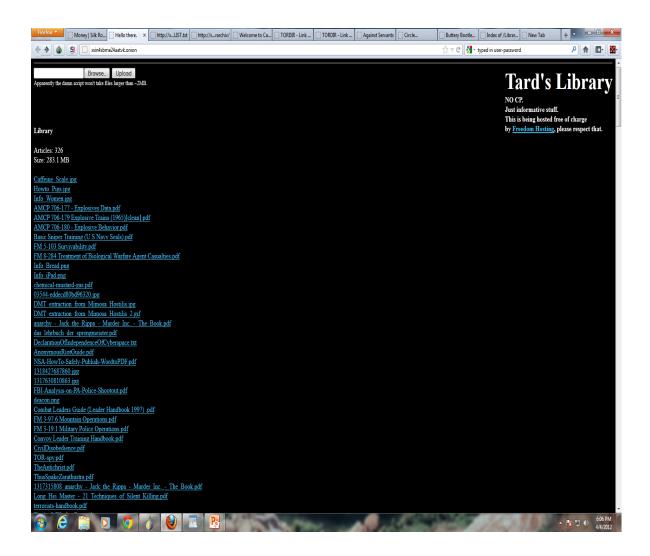
- Dark email: email providers are only accessible via the Tor Browser, an anonymity tool designed to conceal the end users identity and heavily encrypt their communication. Tor is used by an array of people including journalists, activists, political dissidents, government-targets, whistleblowers, the government and just about anyone since it's an open-source free tool.
- ProtonMail protonirockerxow.onion
- Torbox torbox3uiot6wchz.onion
- Bitmessage bitmailendavkbec.onion, clearweb
- Mail2Tor mail2tor2zyjdctd.onion
- RiseUp nzh3fv6jc6jskki3.onion, clearweb
- Cock.li (NSFW) cockmailwwfvrtqj.onion, clearweb
- Lelantos lelantoss7bcnwbv.onion paid accounts only
- Autistici wi7qkxyrdpu5cmvr.onion, clearweb
- AnonInbox ncikv3i4qfzwy2qy.onion paid accounts only
- **VFEMail** 344c6kbnjnljjzlz.onion, clearweb
- Dead: Sigaint sigaintevyh2rzvw.onion



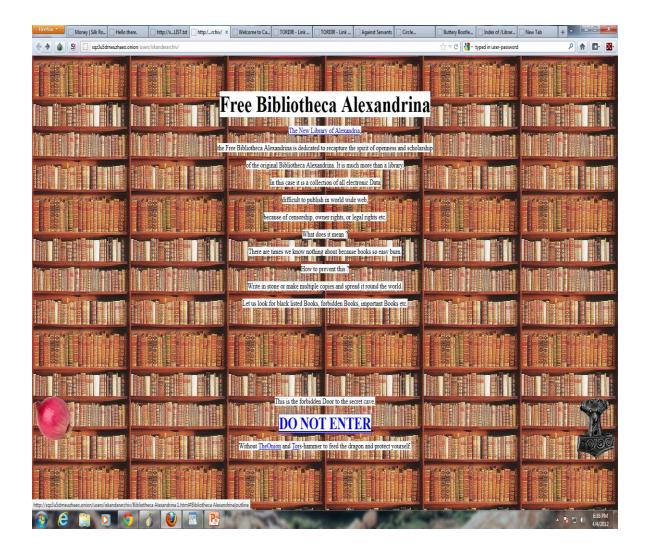
Black Markets: this is an example of one of the many online black markets. This one did not require a paid membership. There are many different ways to spend bit coins, such as on apparel, money transfers, drugs, books, and even digital goods.

🔥 Silk Roa	messages 0 orden	s 0 account B0.00		
anonymous mar				Go
Shop by Category				
Drugs 8,670 Cannabis 2,066 Dissociatives 165 Ecstasy 660 Opioids 591 Other 455				
Precursors 50 Prescription 2,146 Psychedelics 981 Stimulants 1,102	1g MDMA 82%+ High Quality -Made in Germany- B 1.30	50 gr. Crystal MDMA Rocks B 23.33	Valium 10mg/ Diazepam (100 Pills) \$ 2.32	3g XxX AAA QUALITY WEED,AMAZING B 0.98
Apparel 264 Art 127 Biotic materials 1 Books 861 Collectibles 5 Computer equipment 32 Custom Orders 68	KAMAGRA	Jelly (India), 1 week pack TheBen	AMANAS Contractor	Mr. Shab
Digital goods 509 Drug paraphernalia 305 Electronics 77	Kamagra jelly (India), <u>1</u> week pack \$ 0.98	Honeycomb Wax (85+% THC) Fully Purged \$ 1.45	1 gram × Moroccan Hash × DUTCH QUALITY \$0.27	Citalopram 10x 20mg table
Erotica 540 Fireworks 2 Food 9 Forgeries 81 Hardware 23 Herbs & Supplements 8 Home & Garden 8	Litter Reterrine Special K	FinestKiwiBuds	1	Accelur laur + 1.9.
Jewelry 54 Lab Supplies 71 Lotteries & games 77 Medical 57	10 grams ketamine crystals \$7.15	[3g] Greenstone NZ Hash (B Grade) <mark>\$</mark> 2.49	+++ 100 x 25i-NBOMe Strawberry Snuff Caps +++ \$3.80	300x 25i/25c-NBOMe Liqui Dropper 1200µg ₿ 4.14

Unthinkable Content: this is an example of someone's own personal page, with content picked out due to it's controversial nature. Here you can find anything from banned readings, to Tre felling. There is content on making one's own explosives, and different many military type documents and guidebooks



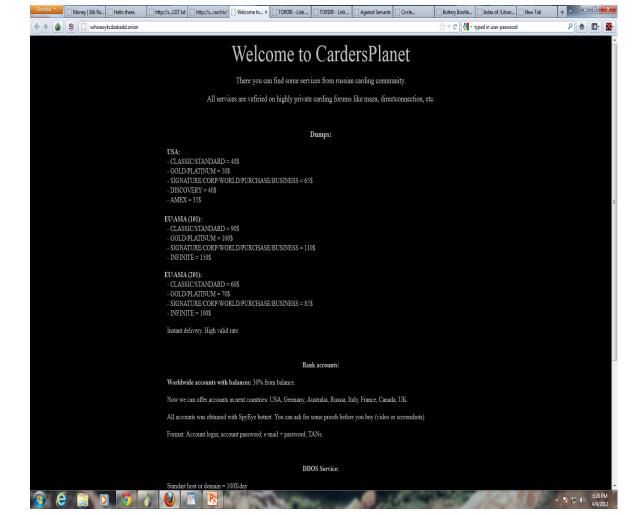
Not Malicious Content: there is a huge portion of the Deep Web that is not malicious at all. This is a huge database of banned, black listed, and forbidden books which you can read and download. Books have been burned in the past and banned for their controversial subject matter, and this is a way for history to be preserved.



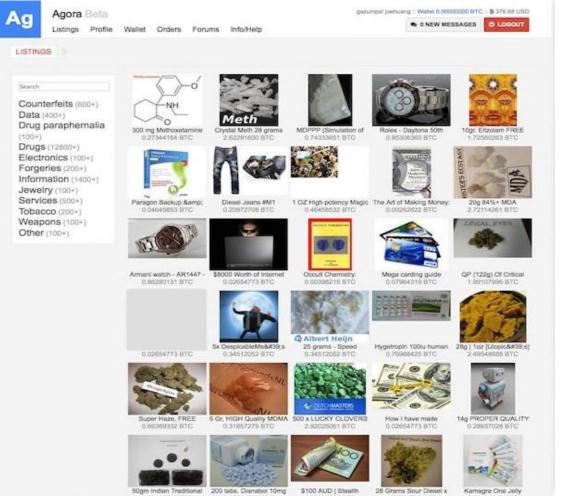
Database: another scholarly database, this .onion site is a compilation of financial, business, real estate, and even marketing tools and texts free to anyone who wants to download them. The Deep Web is a great archive for educational material.

Firefox *	Money	Silk Ro	Hello ther	http://xLIST.txt http://xrarchiv/ Welcome to Ca TORDIR - Link TORDIR - Link Against Servants	ircle Buttery Bootle Index of /Li × New Tab	+ -
€€) S 🖸	am4wuhz	3zifexz5u.oni	/Library/English/Business/	🏫 マ 🕑 🚷 י typed in user-password	۹ 🗈 🗗
ndor	of /Libra	/E	aliah/D	in in each		
nuex	OI /LIDIA	гу/Еп	gusu/d	511055/		
ode li	nks bytes	last-ch	anged na	e		
rw- 1	141450	4 Mar	3 2008	Ebook) - David Frey - The Small Business Marketing Bible 2003 (312 Pages).pdf		
rw- 1	491200	5 Mar	3 2008	Ebook) Harper Business - Stock Market Wizards (Jack Schwager).pdf		
rwx 4		B Dec 2				
rwx 78		8 Jan 2				
rw- 1 rw- 1			3 2008 3 2008	.04.FinancialFitness.pdf		
rw- 1 rw- 1				HiddenPsychological.pdf enjamin Graham - The Intelligent Investor investing + found at redsamara.com.pd		
rw- 1			3 2008	rands.That.Rock.What.Business.Leaders.Can.Learn.from.the.World.of.Rock.and.Roll		
rw- 1		4 Mar		usiness Blogging Toolset100 Internet Resources for Entrepreneur-Writers.pdf		
rw- 1	1947999	6 Mar	3 2008	RM McGraw Hill - Customer Relationship Management (2002).pdf		
rw- 1	2355	2 Mar	3 2008	consulting-Ten Commandments of Small Business [Lesson].doc		
rw- 1		3 Mar		avid Frey - Business - Six Deadly Small Business Marketing Secrets.pdf		
rw- 1		0 Mar		ionald Trump - Fortune Without Fear Real Estate Riches.pdf		
rw- 1	00001		3 2008	book -en- Cooking- Jamie Oliver - The Naked Chef 2 Cook Book.pdf		
rw- 1		8 Mar		conomics - Freakonomics - A Rogue Economist Explores the Hidden Side of Everyth		
rw- 1 rw- 1		s Mar 3 Mar	3 2008	ather to Son.pdf inance Investment - The Global Money Markets.pdf		
cw- 1 cw- 1		s Mar 8 Mar		inance investment - The Global Money Markets.pdf inance Investment - Trump Strategies for Real Estate.pdf		
rw- 1		6 Mar		inance investments 5th Ed - Z Bodie, A Kane & A J Marcus (McGraw-Hill) - 2001.p		
rw- 1			3 2008	'inance Management Project Strategic - Handbook for small business.pdf		
rw- 1			3 2008	inance, Investment, Stock, Trading - Soros Unauthorized Biography.pdf		
cw- 1	720575	1 Mar	3 2008	ive-Minute Mba In Corporate Finance.pdf		
rw- 1	337105	0 Mar	3 2008	arvard Business Review - How information gives you competitive advantage - Mich		
cw- 1			3 2008	arvard Business Review - The 5 Stages Of Small Business Growth.pdf		
rw- 1		2 Mar		arvard Business Review - What Is Strategy - Michael Porter.pdf		
rw- 1		8 Mar		arvard Business Review - Why Good Companies Go Bad.pdf		
:w- 1 :w- 1		6 Mar 5 Mar		arvard Business School Press - Blue Ocean Strategy (2005).pdf arvard.Business.Press.Blue.Ocean.Strategy.2005.pdf		
		2 Mar		elping Small Business Owners and Self-Employed Professionals Do More With Less.		
rw- 1			3 2008	DIOTS GUIDE - Complete Idiots Guide to Small Business.pdf		
rw- 1			3 2008	nside The Guru Mind - Peter Drucker.pdf		
rw- 1	288106	6 Mar	3 2008	nsider's Guide to Trading the World's Stock Markets.pdf		
cw- 1		7 Mar		ohn Wiley & Sons - The 7 Irrefutable Rules of Small Business Growth - 2005.pdf		
rw- 1		4 Mar		ust 1% The Power of Microtrends.pdf		
:w- 1				aplan - The Business Start Up Kit.pdf		
:w- 1			3 2008	aplan Professional - Financing Secrets of a Millionaire Real Estate Investor -		
cw- 1 cw- 1				atz & McCormick 2000 The Encyclopedia of Trading Strategies.pdf		
w- 1			3 2008	earn the Principles of Business Writing.pdf aking A Living From Your eBay Business, 2nd Edition.chm		
w- 1		9 Mar		anaging Your Business with Outlook 2003 for Dummies.pdf		
w- 1		1 Mar		arketing Branding - Defending the Brand - Aggressive Strategies for Protecting		
w- 1		8 Mar		arketing, Planning And Strategy.pdf		
w- 1		5 Mar		ba In Finance.pdf		
cw- 1			3 2008	cGraw-Hill - The Law of Financial Success.pdf		
w- 1		1 Mar		lograw-Hill - Fundamentals Of Managerial Economics.pdf		
w- 1			3 2008	enshikov - Millionaires and Managers - Structure of US Financial Oligarchy (196		
WX 2			4 2008	owerful Sleep Package/		
w− 1 w− 1				eal Estate - Mortgage & Finance.pdf on Paul Fillars of Prosperity - Free Markets, Honest Money, Private Propert		
:w- 1 :w- 1		1 Dec 2		tarting an Online Business for Dummies 4th Edition.pdf		
w- 1		3 Mar		trategic Marketing Handbook.pdf		
rw- 1		4 Mar		trategy and the Internet - Michael Porter (Harvard Business Review).pdf		
w- 1		4 Mar		ao Te Ching.pdf		
rw- 1	52872	1 Mar	3 2008	he Creation of Conscious Culture through Educational Innovation.pdf		
rw- 1				he Financial Analyst's Handbook (Stock Market).pdf		
rw- 1				he Secrets of Market-Driven Leaders & Pragmatic Approach.pdf		
				s/Business Blogging Toolset100 Internet Resources for Entrepreneur-Writers.pdf		

Malicious Content: The Deep Web is full of malicious content. On this Russian-based community hacking website, one can purchase credit card information, PayPal account information, bank accounts, and even the service of DDoSing a website. This is when the website is overloaded with information sent to it, and eventually is forced to shut down.



Agora



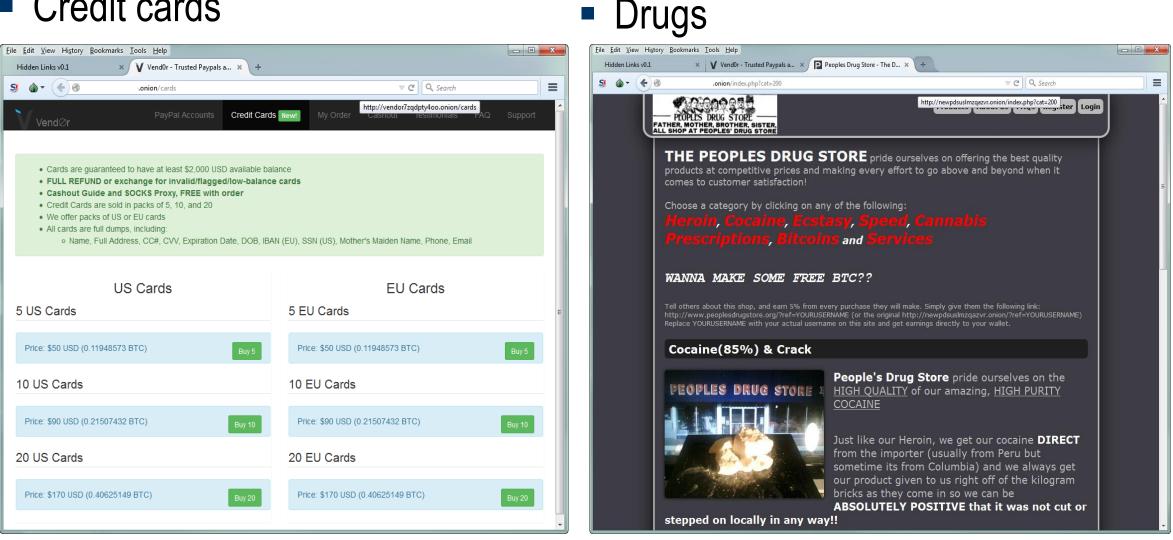
Hidden links

<u>File Edit View</u> H	li <u>s</u> tory <u>B</u> oo	kmarks <u>T</u> ools <u>H</u> elp			
Hidden Links v0.	1	× V Vend0r - Trusted Paypals a × +			
S 💩 - 🗲) 🕲	.onion	⊽ C	Q Search	≡
	UP	Credit Card Vendor - http://clubSue7xcsgingl.onion/ http://hlinkhign4 Verified Credit card selleri Get your cards here!	obv3a3.onion/		^
	Market	lace:		We are still in Beta!	
	UP	AppleTor - http://appleze2rg3on25s.onion/new/			
	33 days	Very good Apple wholesale seller. Good prices and fast shipping! BlackMarket Team - http://blackz5jtkief7mz.onion		1. Lists and Search Engines	
		Reliable supplier with assured service quality!		2. Marketplace	
	UP	Only.Cigs - http://cigs7cviqbi4bvuy.onion/		1. Financial Services 2. Commercial	E
	UP	Contraband with cigarettes, no bullshit, only original blends for Bitcoin! aApple Store - http://gappoos46myl2bwg.onion/		3. Drugs	
		Carded Gadgets with good price - Building a good reputation is one of our core values	- Accept Escrow.	3. Hosting Web, File and Image	
	N/A:	PayPal Vendor - http://vendorfezyqihkf7.onion Automated Machine, MarketPlace of hacked PayPal accounts for 21% of the balance.		4. Warez, Phreak and Anarchy	
	UP	Hidden Apple Store - http://lks3bvfzgdfqpbfa.onion		5. Forums, Boards and Chans 6. Political and Advocacy	
	5 days	Get two Apple computers for the price of one!		7. Email and Messaging	
	UP 5 days	100x Your Bitoins in 24 Hours - http://222222c6hrxbydu.onion Pay 0.01 BTC today, get 1 BTC tomorrow		8. Blogs and Essays	
	UP	Cheap PayPal Accounts - http://2222snt2jjhvlkew.onion		9. Whistleblowing	
	3 days	Buy now your account and go shopping		10. XXX Adult Erotic 18+ 11. Other	
	UP 1 day	<u>No Background Check Gun Store</u> - http://6xbcodgrkz3tffpv.onion More than 1000 guns in inventory		12. Non-English	
	UP	Guns Dark Market - http://gunsjmzh2btr7lpy.onion		13. Off-Line Links	
	1 day	Guns market to buy guns, full auto assault rifles, pistols, grenade launchers			
	Financia	l Services:			
	UP	Bitcoin Fog - http://foggeddriztrcar2.onion/			
	33 days	Bitcoin Laundry Sistem. The service takes 1%-3% (randomized for obscurity). C'thulhu Resume - http://cthulhuuap7ch47k.onion/			
		Permanent Solutions to Common Problems!			
	UP	Shadow Wallet - http://shadowcbzen24qda.onion/			
	33 days	An anonymous user friendly bitcoin wallet. Old Man Fixer's Fixing Services - http://c2ad575g6coldman.onion/index.html			
		The internet's one stop shop for all things illicit and devious.			
	UP	A BTC X 10 A - http://btcxxlq2p3azq6go.onion/			
	5 days	Multiply your Bitcoins by 10 between 10 minutes and 24 hours! BTC x 100 in 6 hours! - http://btchambzl63m22va.onion			
		Get your BTCs back x 100 within 6 hours.			
	UP	Tumbly, low fee Bitcoin tumbler - http://tumbly5lisxnjozd.onion/			
	5 days N/A:	Get clean bitcoins with low fees, cheap, reliable and fast! BitExploitions - http://qx2xyhtp6on7gtns.onion/			
	IN/A: 1d Oerr	The Original BitExploitions - Multiply Your Bitcoin			
	UP	BTC x 100! the real (mirror 2) - http://btcgaop6gqxagxge.onion			
	5 days UP	Get your BTCs back x 100! within max. 6 hours. [Proof included]			
	UP F I	Verified Card Vendorl - http://54ogum7gwxhtgiya.onion/insertor/view/df71ec94			-

D 73006265 BTC D 13404821 BTC 0.292025

0.29202506 BTC 1.02739726 BTC 0.01194647 BTC

Credit cards



Internet of Things Security ++

IoT: is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or humanto-computer interaction. the Internet of things has evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems.





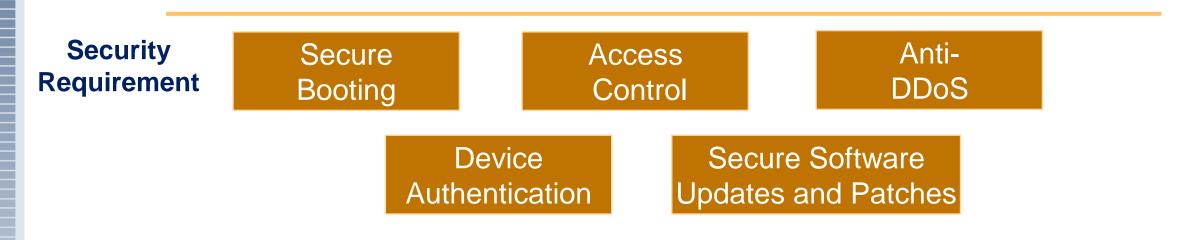
IoT Attacks Level3 outage map



October 21, 2016, DDoS attack to Dyn's Managed DNS infrastructure.



In 2014, remote code execution vulnerability, affected more than 150000 Webcam devices, because of weak password.



4 Layers Model of IoT

Layers

Integrated Application









Information Processing

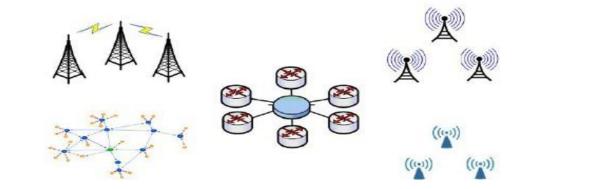








Network Construction



Sensing and Identification

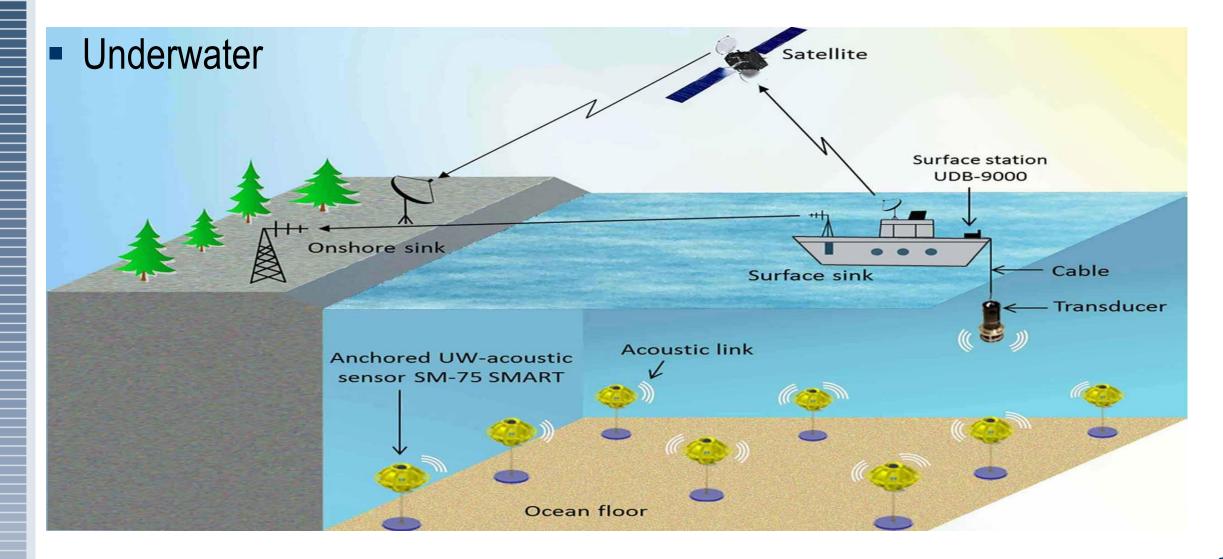




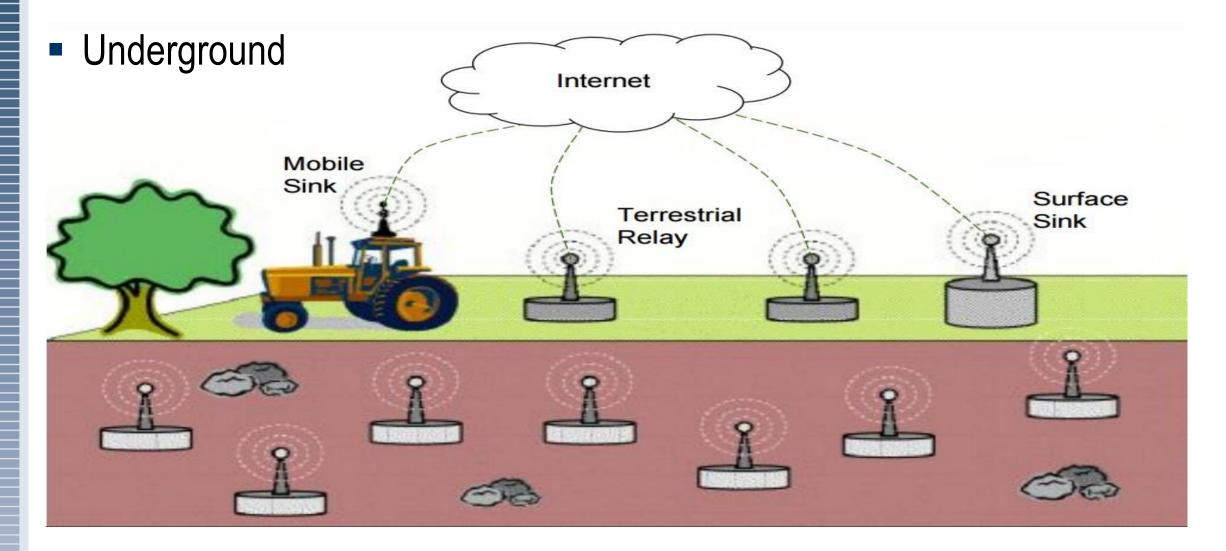




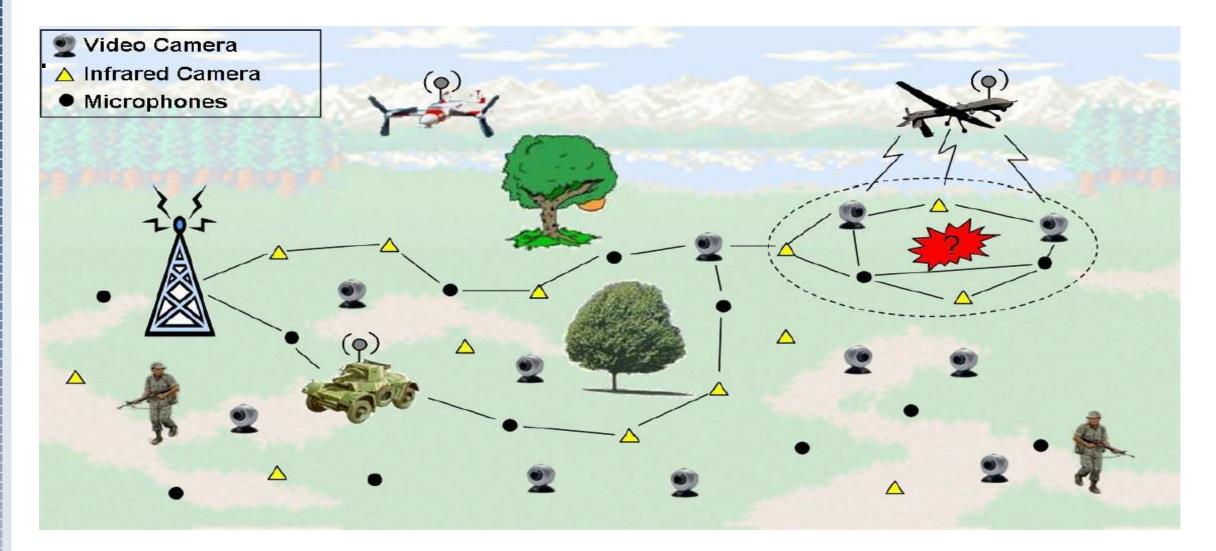
Internet of Underwater Things



Internet of Underground Things



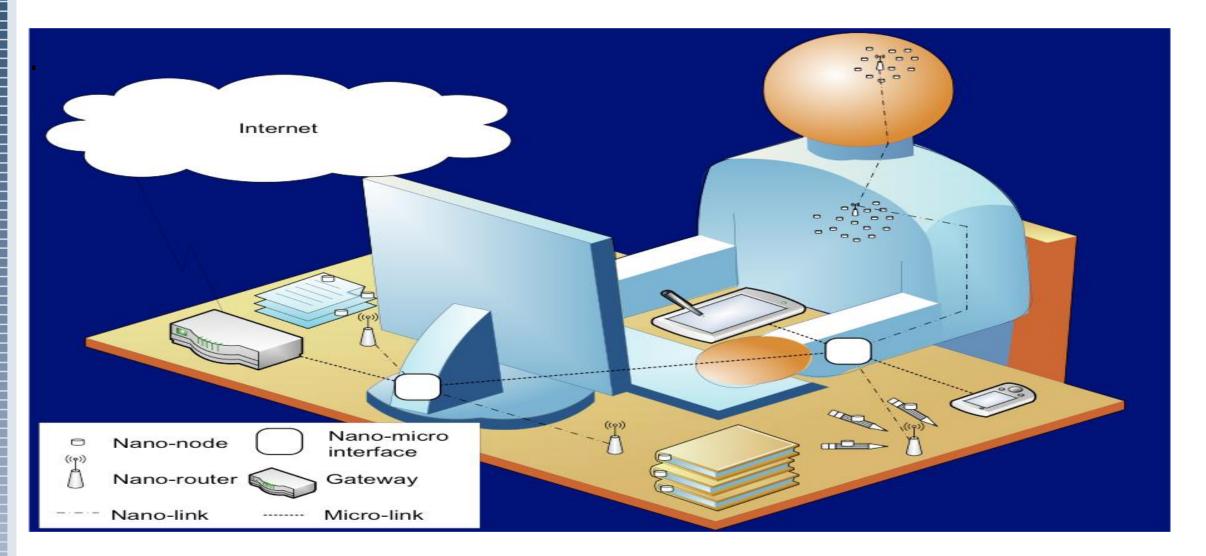
Internet of Battlefield Things



Internet of Space Things



Internet of Nanothings



Internet of Bio-Nanothings

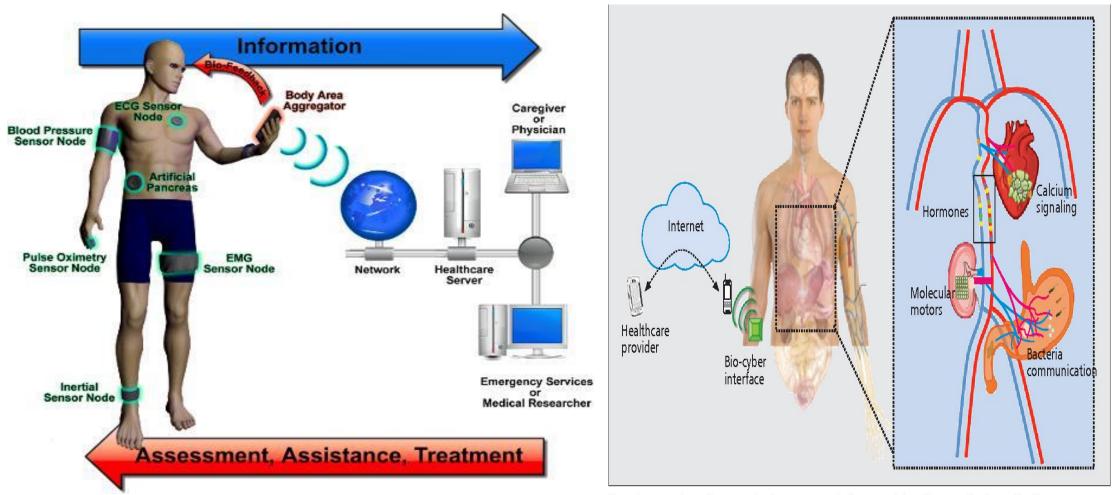
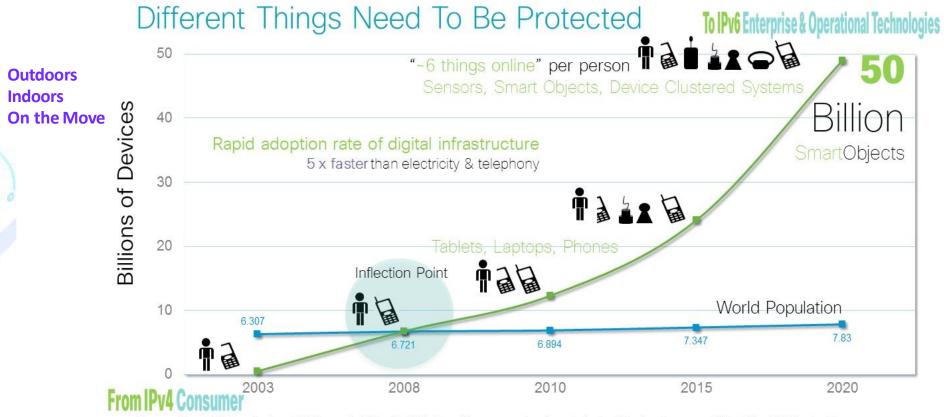


Figure 4. Network architecture for the Internet of Bio-NanoThings for Intra-body applications.

Internet of Things: Perspectives

•

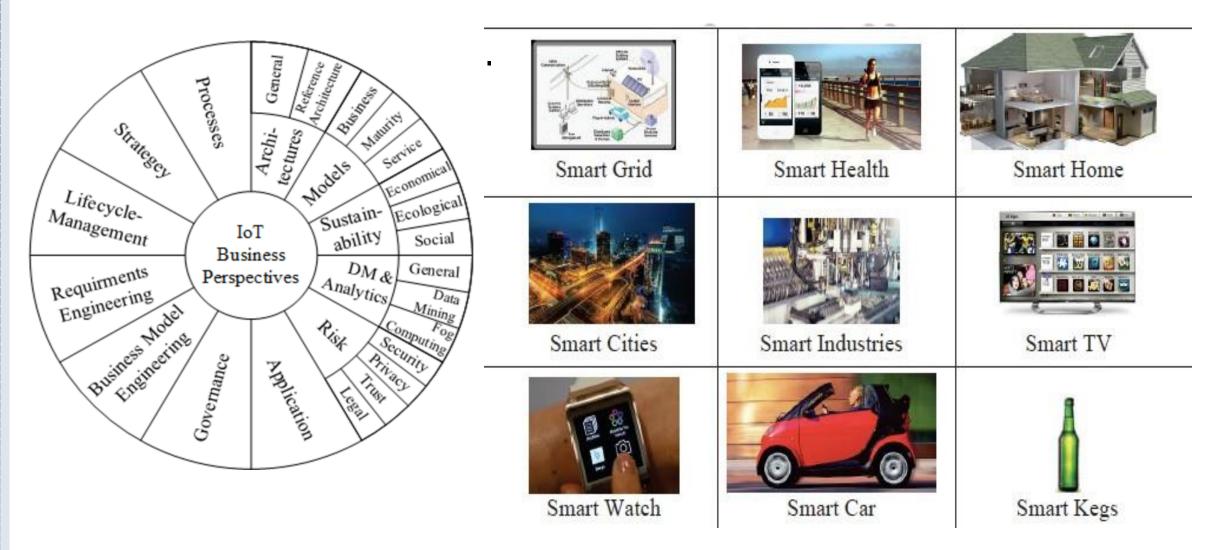
- On the Move
- Outdoors and Indoors
- Nights and Daytime



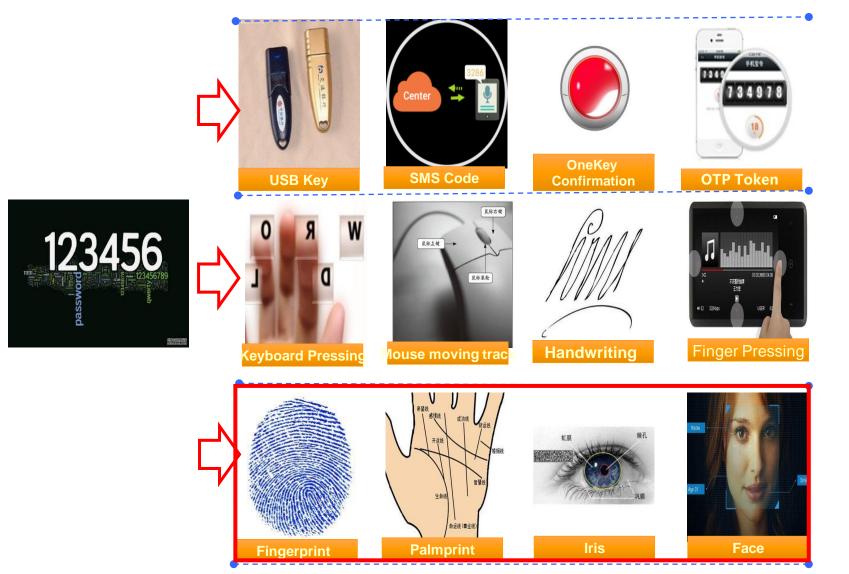
- Human to Human (H2H)
- Human to Thing (H2T)
- Thing to Thing (T2T)

Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf

Top Industries for IoT development



Stronger Authentication



Web API for "Human ontology authentication" ?

> Advantages (1)Portable (2)Secure (3)Stable (4)Unique (5)Universal (6)Convenient (7)Collective (8)Acceptable



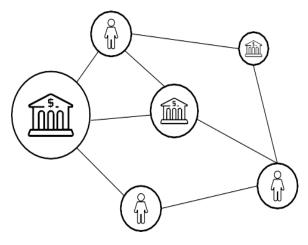
The Internet of Blockchain +++

Inter Blockchain Communication (IBC): The Cosmos Network has the Inter Blockchain Communication (IBC) protocol to allow blockchains to interact with other blockchains. The network of blockchains will communicate through IBC, with the Cosmos Network as the central hub. Blockchains are connected in a hub and spoke model to the Cosmos Hub. The spokes of the network are called Zones, as seen in the diagram.

Ethereum $(\mathbf{0})$ endermint Consensu CØSMOS INTERNET OF BLOCKCHAINS

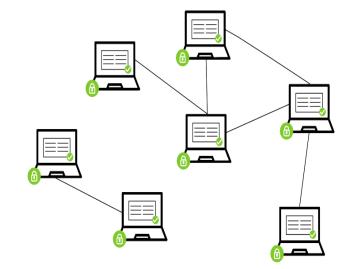
Block Chain in Brief

Current Financial System



- Central authorities (bank, fed, notary, escrow, etc.) transfer actual value between two parties.
- Multiple intermediaries and recordkeeping are required to facilitate transfer of assets and create trust

BlockChain System



- Distributed network of computers (nodes) that maintain a shared source of information
- Transaction data is immutable
- Peer to Peer transactions using digital tokens to represent assets and value

Bitcoin vs Block Chain

Bitcoin

Bitcoin is a digital cryptocurrency made up of processed data blocks used for online and brick-andmortar purchases. Because bitcoins are limited and their value is determined by market forces, bitcoins are also traded like stocks on various exchanges.

- A digital currency which was in a lot of ways the first demonstrable use of BlockChain
- A protocol that supports a decentralized, pseudo-anonymous, peer-to-peer digital currency

BlockChain

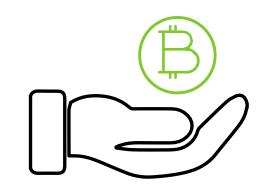
A digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network. "Blocks" on the blockchain are made up of digital pieces of information. Specifically, they have three parts

Blocks store information about transactions.

Blocks store information about who is participating in transactions.

Blocks store information that distinguishes them from other blocks.

- Distributed
- Secure
- Log file



Blockchain (cont'd)

A **BlockChain** is a distributed secure log file or **shared ledger** with technology to trust transactions without a central authority

A shared ledger technology allowing any participant in the business network to see the established (via distributed consensus) system of record (ledger)

Each peer address is anonymous and multiple addresses may map to the same transactor

Every viable transaction is stored in the shared public ledger

Transactions are placed in **blocks**, which are linked by **one way hashes**

Operates in a **peer to peer mode** and is mostly based on DNS and "**seed nodes**"

Blockchain (cont'd)

- BlockChains are essentially facilitated on a platform of distributed databases with some inbuilt pre-agreed technical and business logic criteria, kept in sync via peer-to-peer mechanisms and pre-agreed consensus algorithms. These are the BlockChain Ledgers.
- Data stored on BlockChains are considered Immutable. Immutable means that something is unchanging over time or unable to be changed.
- In a BlockChain context, once data has been written to a BlockChain no one, not even a system administrator, can change it. This provides benefits for audit.
- With respect to immutability, the way the data is structured is significant. There are two key ideas: Hashes and Blocks.

Blockchain (cont'd)

• Keeping Secure Records:

- Records and validates each and every transaction made in a cryptographic manner
- Multi-Signatures
- Encrypted Communication
- True Non-Repudiation: Transaction un-linkability while incorporating identity management/ auditability

Efficient Value Transfer:

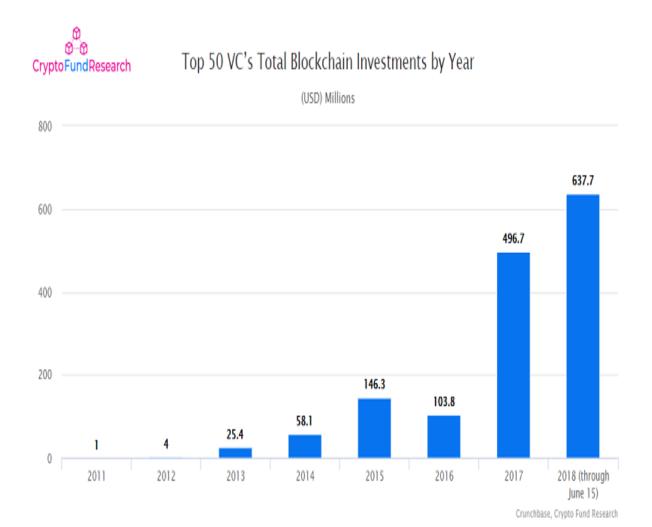
- BlockChain mining discards the need of any third-party or central authority for P2P transactions needed to transfer value between two parties: Process and Cost Efficiency;
- Reduced internal risks;
- Mitigate Man in the Middle

Smart Contracts:

- Decentralization of the technology and distributed Ledger for smart contracts development, exchange and signature.
- Transfer over Internet by anyone with computer or smart phone

Blockchain Challenges

- BlockChain significantly alters the need for trusted third-party authentication through a financial institution
- Challenges of legacy infrastructure
- Challenges in understanding the technology
- Complex cryptosystems
- Decentralized cryptosystems
- Attacks on Cryptosystems
- Government backing and standards are currently in exploratory phase only
- Can facilitate money laundering, crime
- Currently cannot support a large number of transactions and is not fast enough



Blockchain players

PLATFORMS	WVODWS Azure	ethereum CREDITS	fact n Blockstack.io	1 🛟 Dig Sig	gital Asset Holdings	CYPHER	symbiont	Blockstream Consensys
WALLETS	xapo	trucain	🛢 coinba	se 🛡 Bit	Go. Ogen		BLOCKCHAIN	CIRCLE
IDENTITY	onename	-	🥑 A9	SET TRAD	DING Serica	V oat:	z clear matics	C everledger
EXCHANGES		coinsetter	r i	BITSTAMP	coin	×	itBit	мкrакеп
PAYMENT PRO	CESSORS	💥 Bitnet		bitpay	Goco	194	₿	🛢 coinbase
LOYALITY & G	IFT CARDS	lowal	gyft H	ARDWARE	BitFur	y KnCM	liner 🕠	Storj.io
PAYMENTS &	REMITTANC	ES •\$	ripple	🔘 CIRCLE	REBIT	stellar	GBitspar	k ABRA
CONSORTIA, VO	s & ORGANI	ZATIONS	R	() ()	HYPERLEDGER PROJEC	r	coolo	

Barriers to Blockchain

- Recording certain types of transactions in a public ledger may be disallowed in a given country because of privacy laws.
- Access to confidential data may be restricted within a permissioned BlockChain
- A public Blockchain may include one-way hashes of confidential data, where access to that data is controlled; the database(s) containing such data can be (partially or totally) purged, if necessary.
- BlockChains can be made interoperable with legacy systems such as credit card processing (vulnerability?).

2) Videos: Discussion & Reflection



- What We Learned From Stuxnet
- Cyber warfare: Legal experts and programmers search for solutions
- Cryptocurrencies in the darknet
- Surface web, deep web, dark net explained
- Darknet Market

Go to the virtual room, and complete the activity thread.



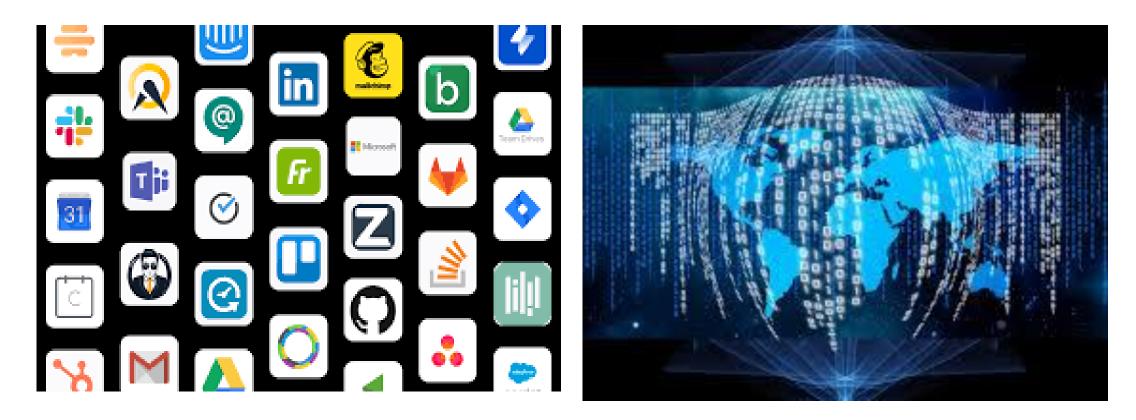


Please go to the Virtual Room for Instructions\\



4) Economics of Cybersecurity

 Markets: Companies and consumers participate in markets, where they exchange goods/services for money or something of value.



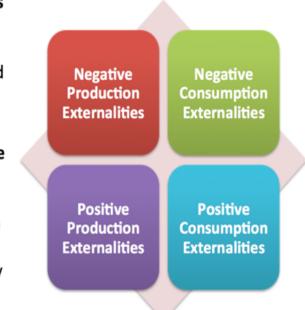
Market Externalities

- Consequences of a transaction or decision that affect someone else who wasn't part of that transaction
- Pollution is a classic example: decisions are made to maximize profit, so in the absence of a legal requirement to deal with pollution, companies don't

Externalities and Market Failure

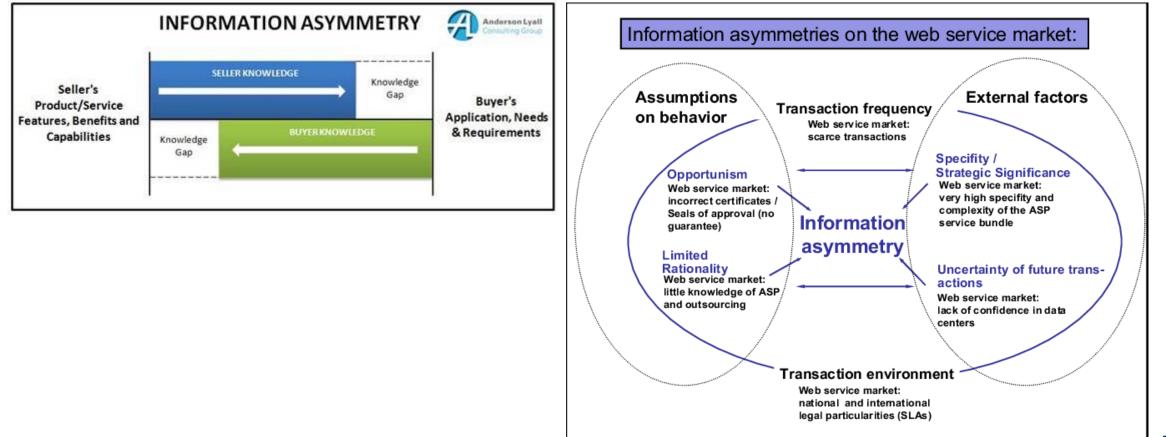
Externalities are a major cause of market failure and occur in nearly every market – be clear on effects for producers and consumers

- Externalities are spill-over effects arising from production and consumption for which no appropriate compensation is paid
- Externalities lie outside the market transaction
- Externalities cause market failure if the price mechanism does not take account of the social costs and social benefits of production and consumption
- Externalities can be positive and/ or negative



Market Information asymmetries

 One actor has information that another actor doesn't have, giving that first actor an advantage



Rationality

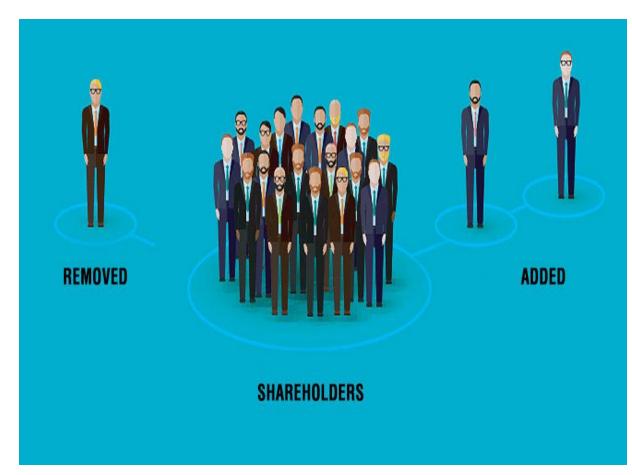
- You pick the option that maximizes your value function (either reduces cost or maximizes profit)
- You make the decision that takes into account the information you have and the shape of the problem
- If intrusion detection system A costs twice as much as intrusion detection system B, but A is not twice as good as B, B is a better value for money.
- Why might you pick A anyway?

Concept of Rationality

DEFINITION OF RATIONALITY The word rational derives from Latin word ration which mean ,**reason**, or **computation** From the economics point of view rationality guide the people to make good choices or decision

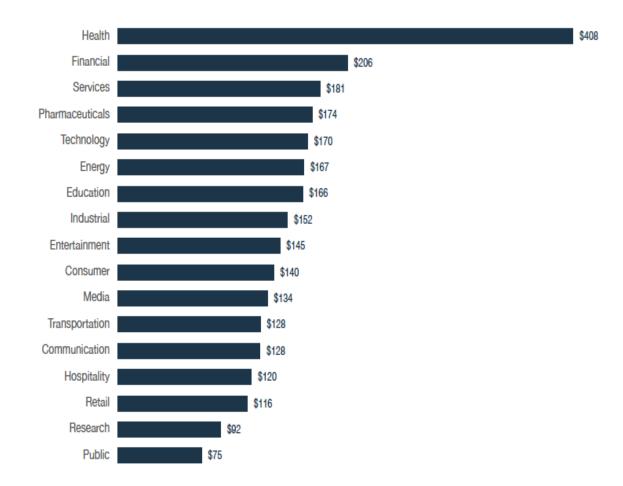
Maximizing shareholder value

- One metric that businesses may use for making these kinds of decisions is whether it will improve their stock price
- That means that you pay people as little as possible and sell your products for as much as the market will bear, as long as the share price increases
- This philosophy means that you don't buy an intrusion detection system unless you as a company will have your share price hurt by a breach.



Cybersecurity Investment

Cost of a data breach per industry per record: <u>https://www.ibm.com/security/data-breach</u>



Critical moments in security

Cyber hygiene addresses ~80% of threats: Cyber hygiene refers to steps taken by users to maintain the health of their computers and devices and improve online security to prevent the theft or corruption of data. Further, as with personal hygiene, cyber hygiene should be practiced regularly to ward off common threats and the natural deterioration of devices and systems.

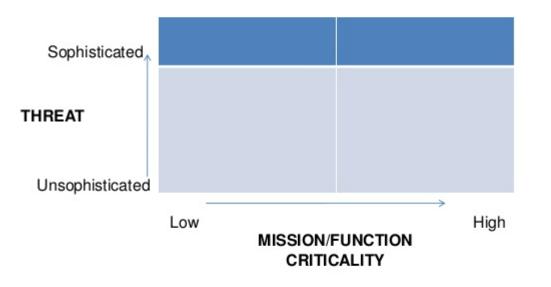
- Good cyber security costs less (and improves operational availability)
- Achieving good hygiene is not a technical issue, rather a Cultural one.
- resistance is very strong and IT prefer to focus on the high end threats

Addressing the 20% "gap" requires a fundamentally different approach:

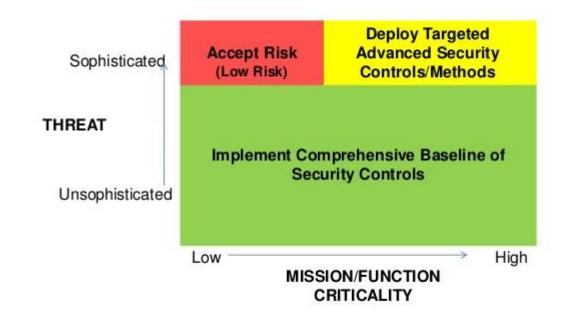
 Some things are counter cultural in consciously accepting risk or partitioning cyber environments (other than by classification)

A foundation

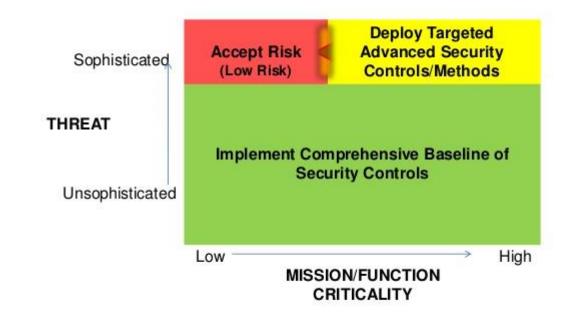
Foundation for Cybersecurity Framework



The Cybersecurity Economic Framework



Reducing Risk Acceptance



Expanding the Baseline of Security Controls

Enhanced Descriptor	Employment of Security Controls	Security Tailored to Mission	Participate in Information Sharing (threat and vulnerabilities)
Managed	CSC Integrated and Continuously Monitored	Partially Mission Focused	Respond to Information Inputs
Performed	Foundational/ Critical Security Controls (CSC) Implemented	Mission Agnostic	Inconsistent Response to Information Inputs

Expanding Targeted Advanced Security Controls/Methods/Tools

Enhanced Descriptor	Employment of Security Controls	Security Tallored to Mission	Participate in Information Sharing (threat and vulnerabilities)
Resilient	Augment CSC Based on Mission and Threats	Investments are Mission Assurance Focused	Tools and Staff to Response to Shared Threat Information
Dynamic	Augment CSC Based on Mission and Threats	Investments are Mission Protection Focused	Tools and Staff to Response to Shared Threat Information

Extended Cybersecurity Framework

Employment of Security Controls	<u>Security Tallored to</u> <u>Mission</u>	Participate in Information Sharing (threat/vul)	<u>Response to Cyber</u> <u>Threats</u>
Augment CSC Based on Mission and Threats	Investments are Mission Assurance Focused	Tools and Staff to Response to Shared Threat Information	Analytical Capabilities to Anticipate Threats
Augment CSC Based on Mission and Threats	Investments are Mission Protection Focused	Tools and Staff to Response to Shared Threat Information	Capabilities for Rapid Reaction To Threats
CSC Integrated and Continuously Monitored	Partially Mission Focused	Respond to Information Inputs	Respond to Attacks After the Fact
Foundational/ Critical Security Controls (CSC) Implemented	Mission Agnostic	Inconsistent Response to Information Inputs	Respond to Attacks After the Fact
	Security Controls Augment CSC Based on Mission and Threats Augment CSC Based on Mission and Threats CSC Integrated and Continuously Monitored Foundational/ Critical Security Controls (CSC)	Security Controls Mission Augment CSC Based on Mission and Threats Investments are Mission Assurance Focused Augment CSC Based on Mission and Threats Investments are Mission Protection Focused Augment CSC Based on Mission and Threats Investments are Mission Protection Focused CSC Integrated and Contrinuously Monitored Partially Mission Focused Foundational/ Critical Security Controls (CSC) Mission Agnostic	Security ControlsMissionInformation Sharing (threat/vul)Augment CSC Based on Mission and ThreatsInvestments are Mission Assurance FocusedTools and Staff to Response to Shared Threat InformationAugment CSC Based on Mission and ThreatsInvestments are Mission Protection FocusedTools and Staff to Response to Shared Threat InformationAugment CSC Based on Mission and ThreatsInvestments are Mission Protection FocusedTools and Staff to Response to Shared Threat InformationCSC Integrated and Continuously MonitoredPartially Mission Focused Mission AgnosticRespond to Information InputsFoundational/ Critical Security Controls (CSC)Mission Agnostic Information InputsInconsistent Response to Information Inputs

9

Extended Cybersecurity Framework

<u>Enhanced</u> <u>Descriptor</u>	Employment of Security Controls	<u>Security Tailored</u> to Mission	Participate in Information Sharing (threat and vulnerabilities)	<u>Response to</u> Cyber Threats	<u>Cybersecurity</u> <u>Framework</u> Area
Le vel 4: Resilient Operate Through Sophisticated Attack	Augment CSC Based on Mission and Threats	Investments are Mission Assurance Focused	Tools and Staff to Response to Shared. Threat Information	Analytical Capabilities to Anticipate Threats	Additional Investments to
Level 3: Dynamic Able to respond to Sophisticated Attack	Augment CSC Based on Mission and Threats	Investments are Mission Protection Focused	Tools and Staff to Response to Shared Threat Information	Capabilities for Rapid Reaction To Threats	Deploy Targeted Advanced Security Controls/Methods
Level 2: Managed Protection against Unsophisticated Attack	CSC integrated and Continuously Monitored	Partially Mission Focused	Respond to Information Inputs	Respond to Attacks After the Fact	Implement Comprehensive Baseline of
Level 1: Performed Some Protection Against Unsophisticated Attacks	Foundational/ Critical Security Controls (CSC) Implemented	Mission Agnostic	Inconsistent Response to Information Inputs	Respond to Attacks After the Fact	Security "Good Hygiene"

Investment Principles

- Investment Principle #1: Implementation of a comprehensive baseline of security controls that address threats that
 are of low to moderate sophistication is essential and is economically beneficial.
- Investment Principle #2: Focus security investment beyond the baseline controls to counter more sophisticated attacks against the functions and data that are most critical to an organization.
- Investment Principle #3: For sophisticated attacks, an organization should accept the security risk of not protecting functions and data that are of lowest impact to the organization's mission and where cost exceeds benefits.
- Investment Principle #4: The economic benefit of participating in multiple, high quality cyber security information sharing exchanges regarding the dynamic characteristics of sophisticated threats is very high.
- Investment Principle #5: Additional Investments to address sophisticated threats should be specifically tailored to the (evolving) threat characteristics.
- Investment Principle #6: Effective countering of the most sophisticated threats (e.g., Nation State) requires investment in current technology controls and human capabilities to be able to effectively predict and respond to attack patterns. Investment Principles

Portfolios for Cybersecurity

• Natural investment portfolios (from an IT perspective) o Common (shared) infrastructure

- 1. Define standard service level; drive out cost o Back office functions—standardize
- 2. Invest only what needed to support mission o Mission unique capabilities
- 3. Invest in differentiated capabilities

Infrastructure portfolio

- 1. Integrate security and operations—separation drives duplication and reduces security
- 2. Architect (partition) infrastructure/applications/data to align with mission criticality (and evolve)
- 3. Follow economic model for investments—hygiene plus mission focused investments tied to mission criticality •

Back office portfolio

- 1. Decide where to accept risk
- 2. Hygiene plus focused investments in selected areas to reduce risk (e.g., financial, PIA) •

Mission unique capabilities

- 1. Establish desired objective (e.g., Level 3 or 4 on prior scale) for mission partitions/enclaves
- 2. Invest in appropriate capabilities and tools •

Metrics for Enhanced Cybersecurity

Enhanced Cybersecurity Framework Descriptor	Employment of Security Controls	<u>Security Tailored to</u> <u>Mission</u>	Participate in Information Sharing (threat and vulnerabilities)	<u>Response to</u> Cyber Threats
Level 4: Resilient Operate Through Sophisticated Attack	Metric: Capability for real time deployment of controls in response to changing threat profile	Metric: 1) Deployed protection architecture based on assuring mission continuity; 2) Regular exercise of ability to operate through attack	Metric: 1) Robust network of information exchange partners monitored on real time basis; 2) Staff capable of extending threat data to predict threat evolution.	Metric: Established policies and practices as well as experienced staff able to permit real time response to sop histicated threats
Level 3: Dynamic Able to respond to Sophisticated Attack	Metric: Implement threat monitoring capabilities to support identification and deployment of additional controls	Metric: 1) Identification of mission oritical capacities; 2) Deployment of (partial) architecture and controls to protect mission critical capabilities	Metric: 1) Robust network with information exchange sources; 2) Experienced staff capable of rapid response to sophisticated threats	Metric: Organic staff capable of recognizing sophisticated threat and recommending response actions
Level 2: Managed Protection against Unsophisticated Attack	Metric: 1) Ensure baseline controls are consistently applied across the enterprise: 2) Controls are implement with (continuous) automated monitoring with a goal of hourly or single digit minute cycle times	Metric: Formal identification of mission critical capabilities	Metric: 1) Established relationship with one or more information sources for cyber threat and vulnerability information; 2) Standard processes for rapidly responding to threat/vulnerability updates	Metric: Organization staff able to respond after the fact to attack
Level 1: Performed Some Protection Against Unsophisticated Attacks	Metrics: 1) Implement DND Top 4 Controls; 2) Implement some additional CSC or DND 35 Controls	Metric: None	Metric: Threat/Vulnesability Information pushed to organization but inconsistently reviewed or applied	Metric : Attack response prompted from outside the organization

Cybersecurity Insurance

- Why mitigate the cybersecurity risk, when we can try to transfer it?
- Costs of Security
 Cyber insurance Policy
- Security Levels
 We don't care, minimal
- Benefits
 Cyber insurance premiums



Cyber Risk Transference

- Financial Risk of Security Incident.
- Cyber Insurers \rightarrow premium needs to be lower than the difference between the benefit and the cost of security
- Cyber Insurance Market Still Underdeveloped
- Interdependent security (externalities in cybersecurity decisions)
- Correlated risk (i.e. impact of a DDoS attack on economic infrastructure)
- Information asymmetries (zero-day vulnerabilities)

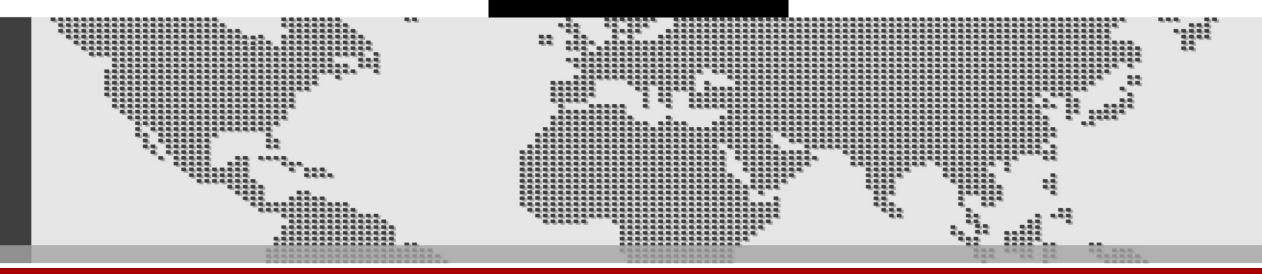
5) In Closing: Debriefings for Cases

- Debriefing for Cases 01 02 03 04
- Please go to the Virtual Room for Instructions
- Prepare your answers accordingly!





Thank you



Day 05

CLOSED FOR BUSINESS

School of Management

and Technology

Business School des SCMT

🗉 ѕмт

Folie • 69

SCMT Steinbeis Center of Management and Technology Research | Education | Consulting El Steinbeis University Berlin SHB

SMT © 2015 | www.scmt.com