
Yesterday
Today
Tomorrow

PROF. DR. JUAN CARLOS BARRERA

CYBER-SECURITY (BC6)

July 2020

Online Germany

Broadcasting from USA

STEINBEIS HOCHSCHULE
School of Management and Technology

Steinbeis HOCHSCHULE

Discovery

Ecosystems of the Cyberspace

Agenda:

1) Cyber-Innovations: Deep Web + + +

2) Videos: Discussion & Reflection

3) Fifth Lab

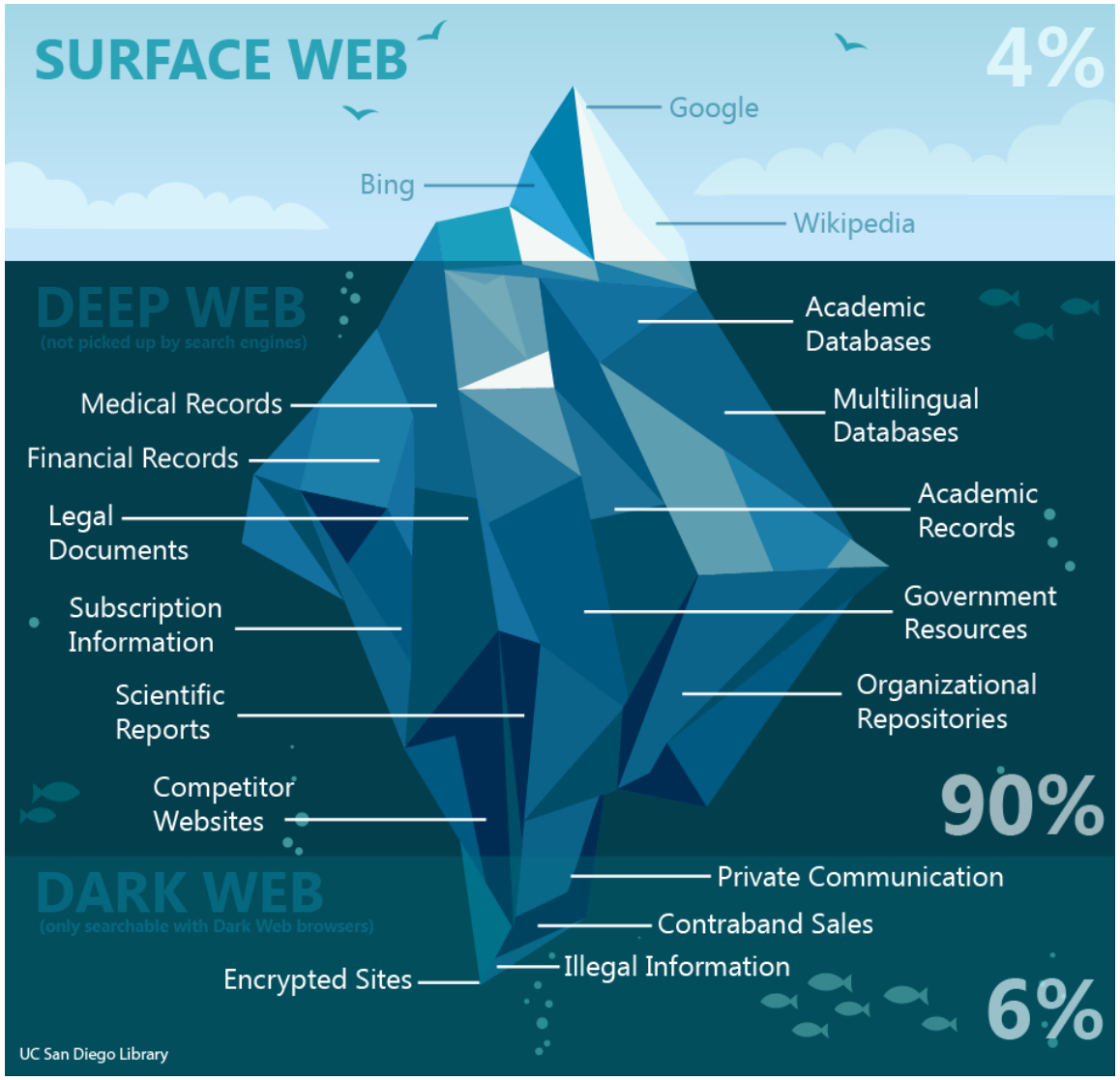
4) Economics of Cybersecurity

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].

History

- 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:

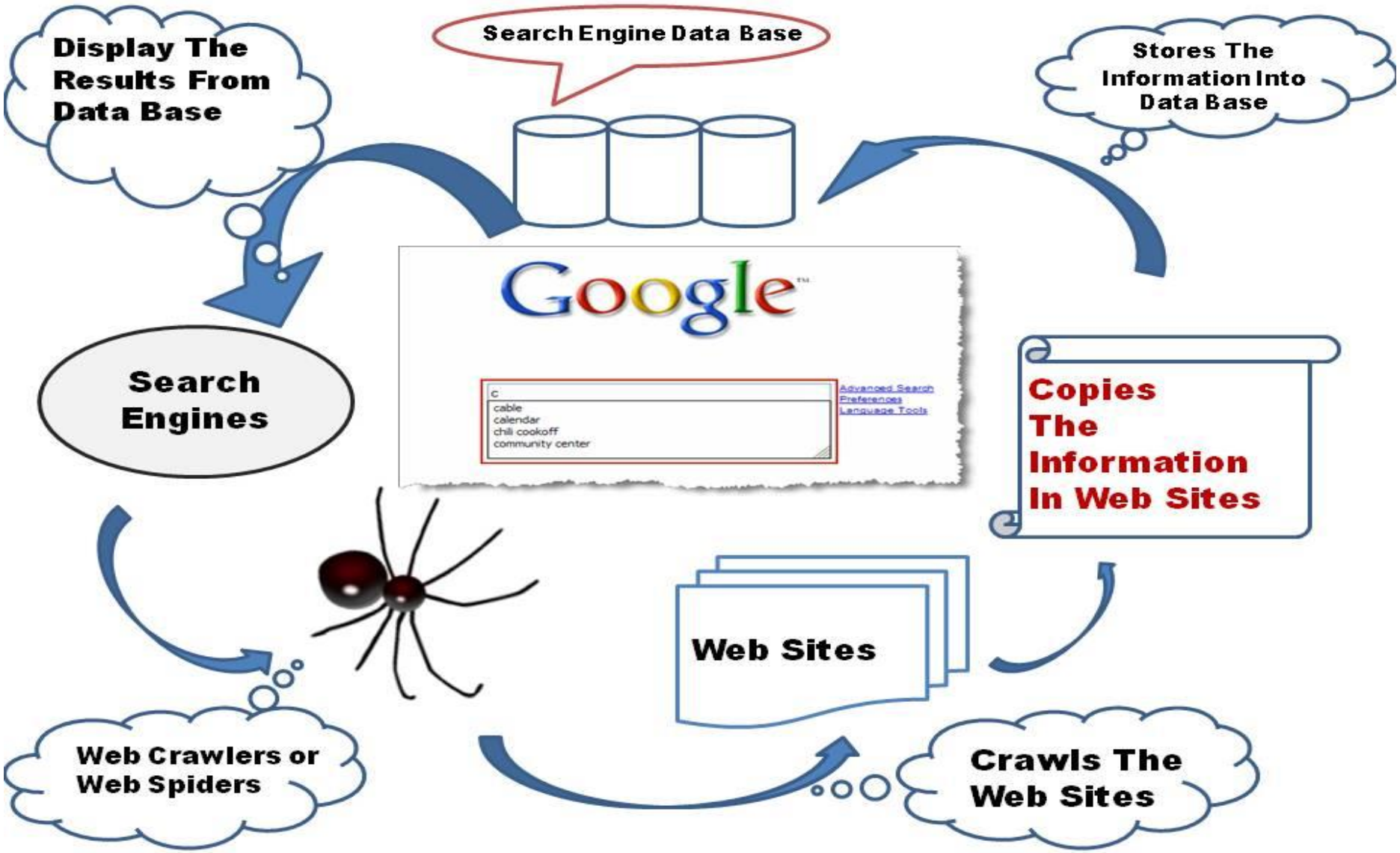
"It would be a site that's possibly reasonably designed, but they didn't bother to register it with any of the search engines. So, no one can find them! You're hidden. I call that the invisible Web".

- 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)

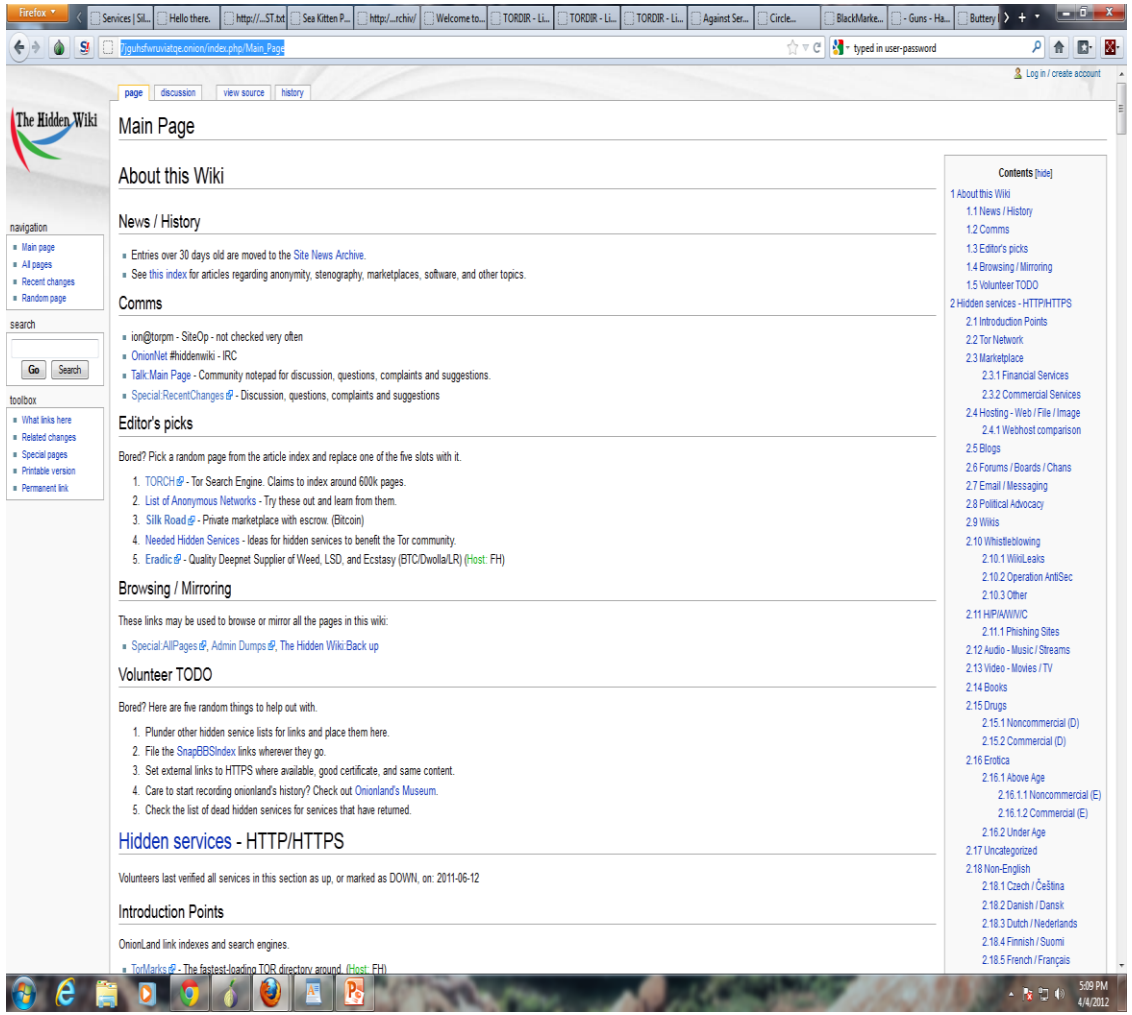
- Tor is software that installs into your browser and sets up the specific connections you need to access dark Web sites.
- Critically it is free software for enabling online anonymity and censorship resistance.
- Onion routing refers to the process of removing encryption layers from Internet communications, 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.

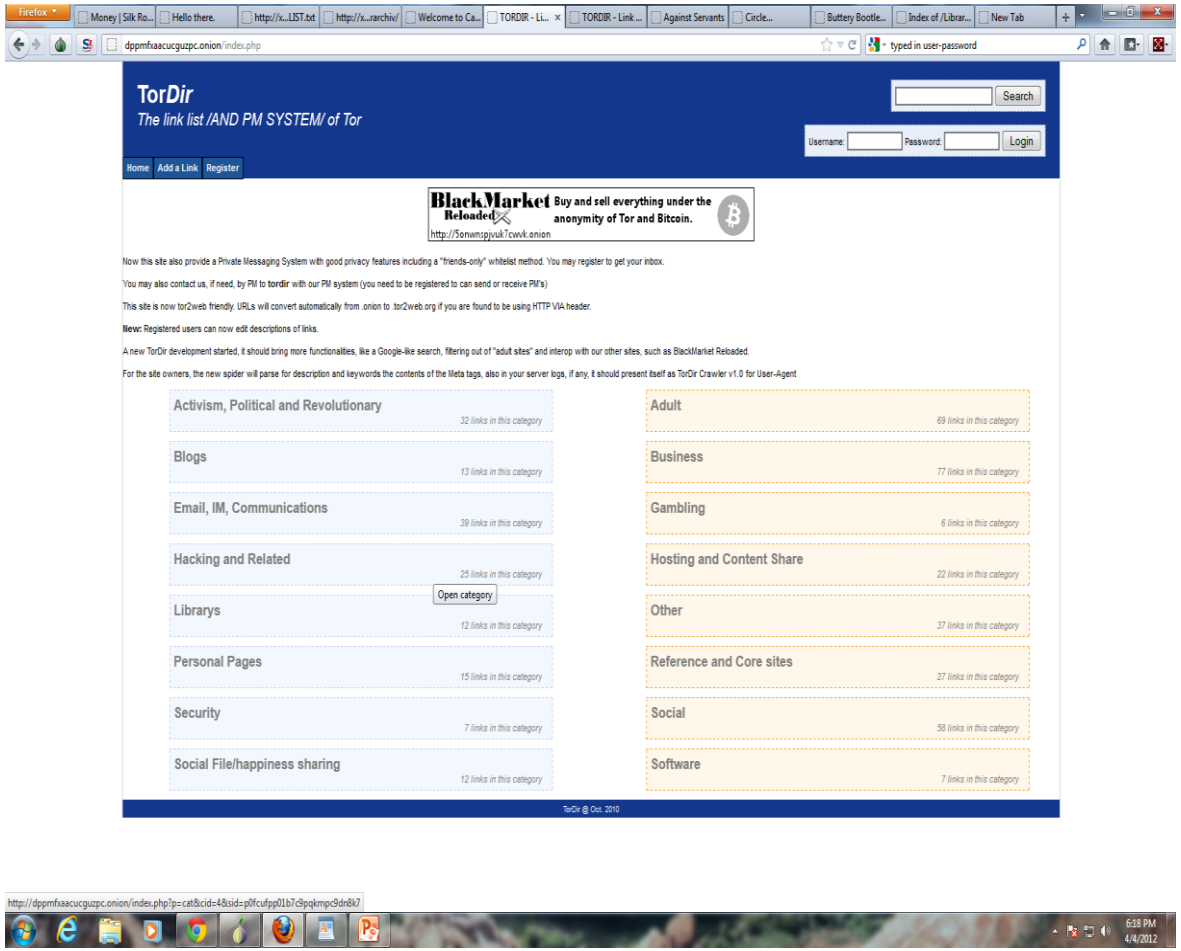
Inside the Deep Web

- 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.



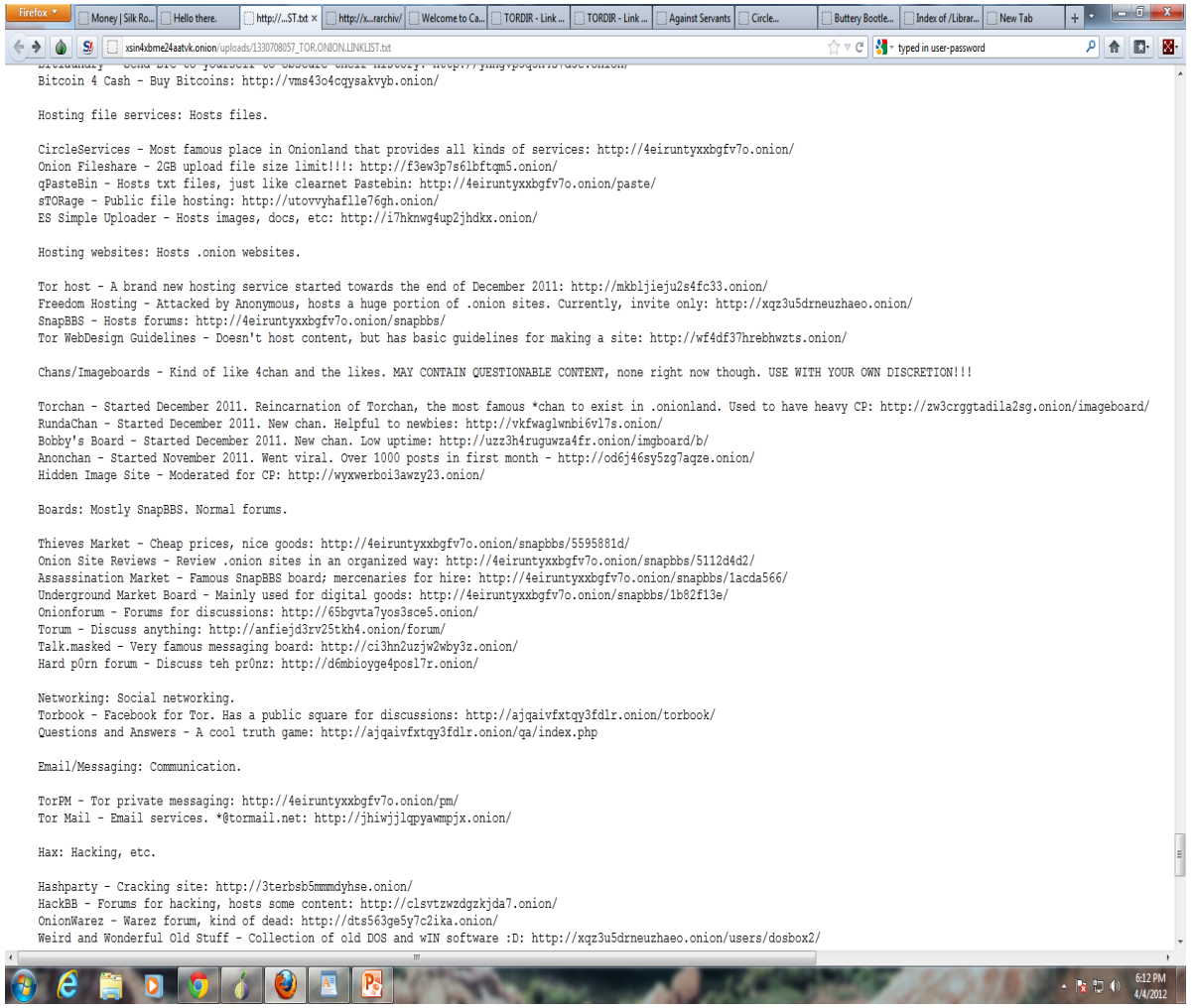
Inside (cont'd)

- 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.



Inside (cont'd)

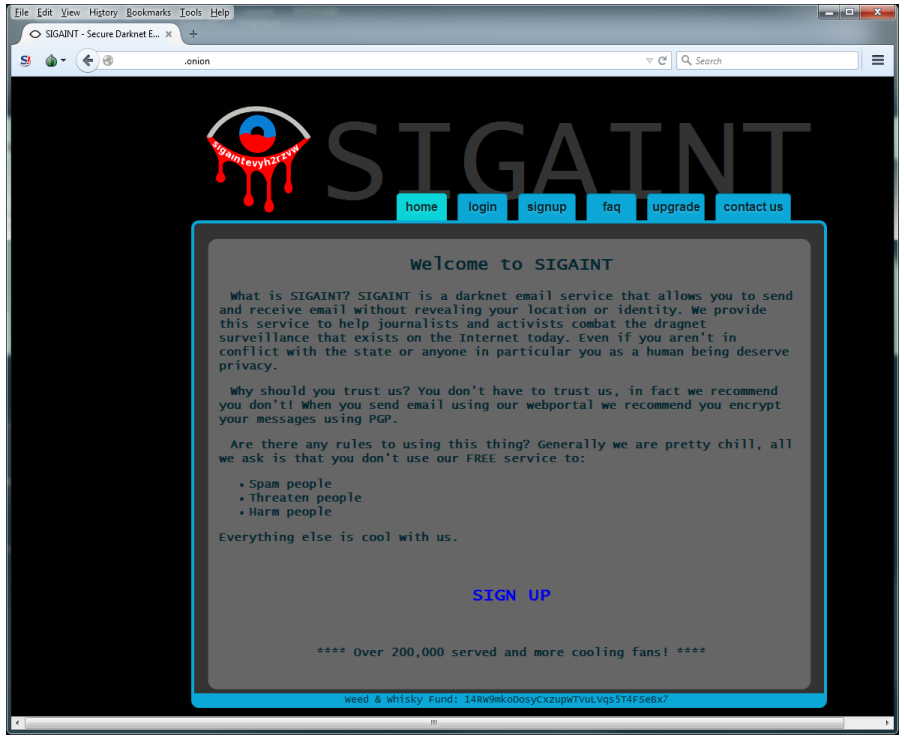
- Through the Hidden Wiki you can find pages like this, which are semi-organized lists of different .onion sites. Many different sites are listed and separated based on function, such as buying/selling/trading, communication, hacking, or intel exchange.



```
Bitcoin 4 Cash - Buy Bitcoins: http://vms43o4cqysakvyb.onion/

Hosting file services: Hosts files.

CircleServices - Most famous place in Onionland that provides all kinds of services: http://4eiruntyxxbgfv7o.onion/
Onion Fileshare - 2GB upload file size limit!!!: http://f3ew3p7s61bftqm5.onion/
qPasteBin - Hosts txt files, just like clearnet Pastebin: http://4eiruntyxxbgfv7o.onion/paste/
sTORage - Public file hosting: http://utovvyhafle76gh.onion/
ES Simple Uploader - Hosts images, docs, etc: http://i7hknwg4up2jhdkx.onion/

Hosting websites: Hosts .onion websites.

Tor host - A brand new hosting service started towards the end of December 2011: http://mkbljieju2s4fc33.onion/
Freedom Hosting - Attacked by Anonymous, hosts a huge portion of .onion sites. Currently, invite only: http://xqz3u5drneuzhaeo.onion/
SnapBBS - Hosts forums: http://4eiruntyxxbgfv7o.onion/snapbbs/
Tor WebDesign Guidelines - Doesn't host content, but has basic guidelines for making a site: http://wf4df37hrebhwzts.onion/

Chans/Imageboards - Kind of like 4chan and the likes. MAY CONTAIN QUESTIONABLE CONTENT, none right now though. USE WITH YOUR OWN DISCRETION!!!

Torchan - Started December 2011. Reincarnation of Torchan, the most famous *chan to exist in .onionland. Used to have heavy CP: http://zw3crggtadila2sg.onion/imageboard/
RundaChan - Started December 2011. New chan. Helpful to newbies: http://vkfwaglwnbi6vl7s.onion/
Bobby's Board - Started December 2011. New chan. Low uptime: http://uzz3h4ruguwza4fr.onion/imgboard/b/
Anonchan - Started November 2011. Went viral. Over 1000 posts in first month - http://od6j46sy5zg7aqze.onion/
Hidden Image Site - Moderated for CP: http://wyxwerboi3awzy23.onion/

Boards: Mostly SnapBBS. Normal forums.

Thieves Market - Cheap prices, nice goods: http://4eiruntyxxbgfv7o.onion/snapbbs/5595881d/
Onion Site Reviews - Review .onion sites in an organized way: http://4eiruntyxxbgfv7o.onion/snapbbs/5112d4d2/
Assassination Market - Famous SnapBBS board; mercenaries for hire: http://4eiruntyxxbgfv7o.onion/snapbbs/1acda566/
Underground Market Board - Mainly used for digital goods: http://4eiruntyxxbgfv7o.onion/snapbbs/1b82f13e/
Onionforum - Forums for discussions: http://65bgvta7yos3sce5.onion/
Torum - Discuss anything: http://anfiejd3rv25tkh4.onion/forum/
Talk.masked - Very famous messaging board: http://ci3hn2uzjw2wby3z.onion/
Hard p0rn forum - Discuss teh pr0nz: http://d6mbioyge4posl7r.onion/

Networking: Social networking.
Torbook - Facebook for Tor. Has a public square for discussions: http://ajqaivfxtqy3fdlr.onion/torbook/
Questions and Answers - A cool truth game: http://ajqaivfxtqy3fdlr.onion/qa/index.php

Email/Messaging: Communication.

TorPM - Tor private messaging: http://4eiruntyxxbgfv7o.onion/pm/
Tor Mail - Email services. *@tormail.net: http://jhiwjjlqpyawmpjx.onion/

Hax: Hacking, etc.

Hashparty - Cracking site: http://3terbsb5mmmdyhse.onion/
HackBB - Forums for hacking, hosts some content: http://clsvtzwzdgzkjda7.onion/
OnionWarez - Warez forum, kind of dead: http://dts563ge5y7c2ika.onion/
Weird and Wonderful Old Stuff - Collection of old DOS and wIN software :D: http://xqz3u5drneuzhaeo.onion/users/dosbox2/
```

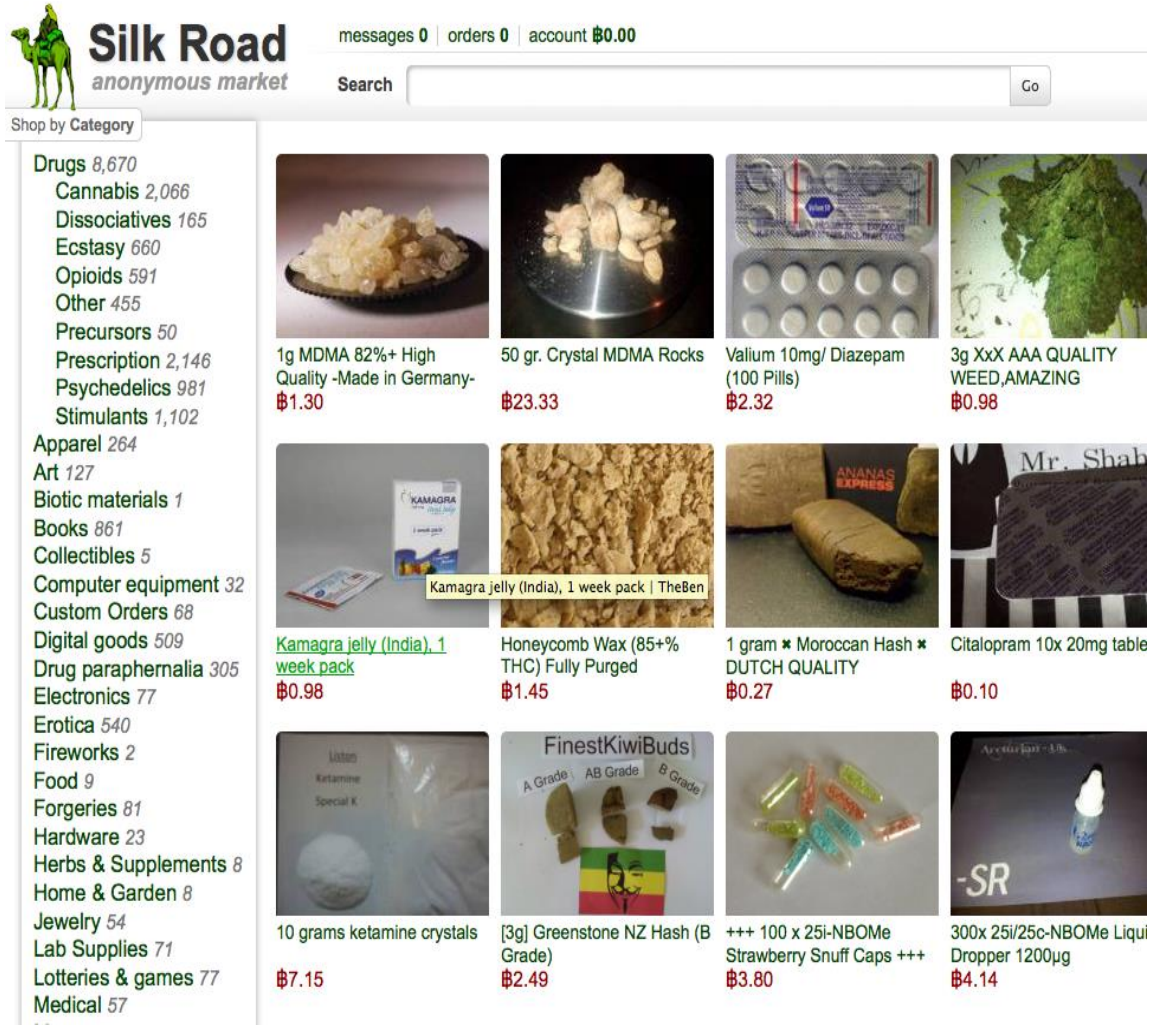
Inside (cont'd)

- **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



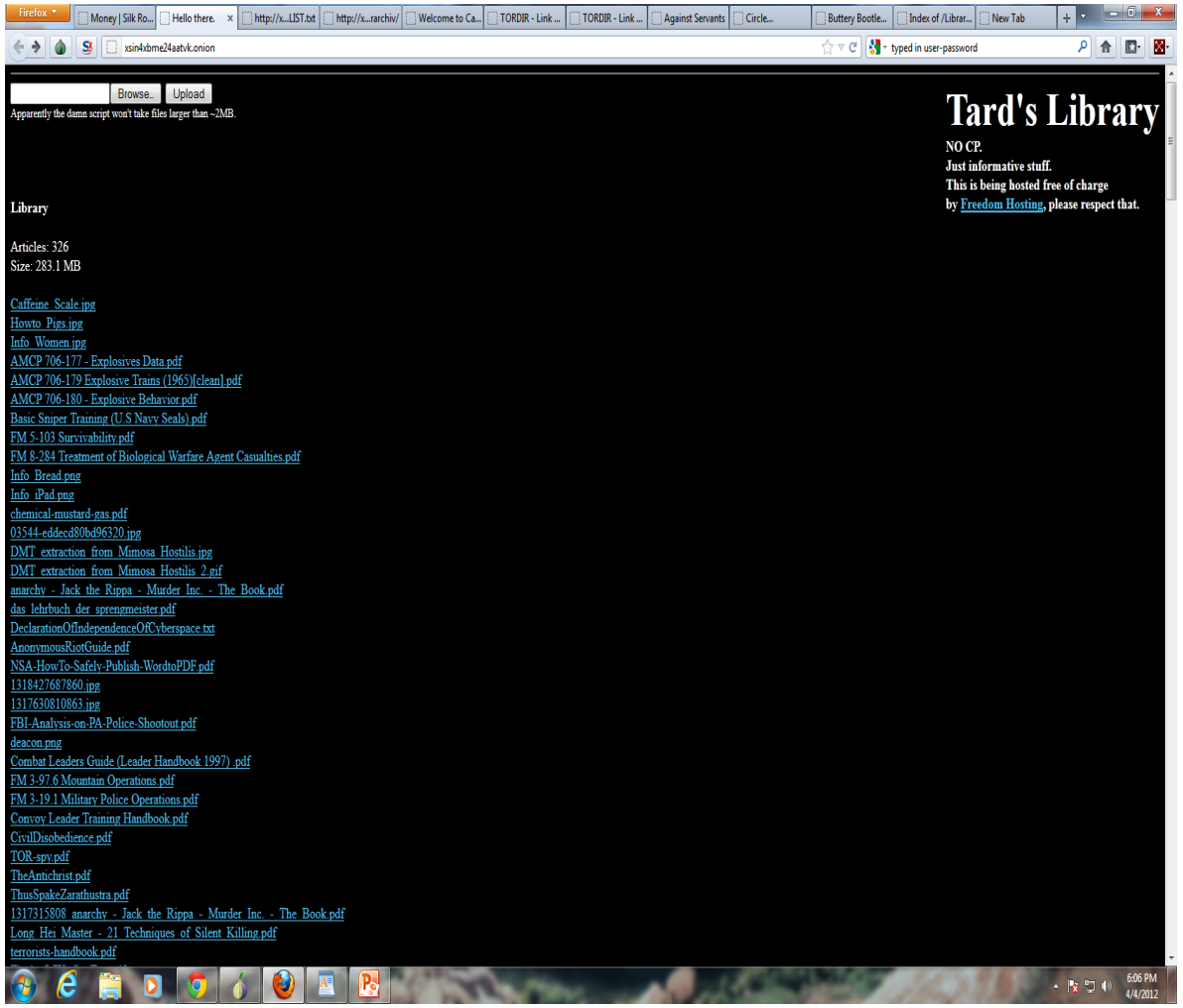
Inside (cont'd)

- 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.



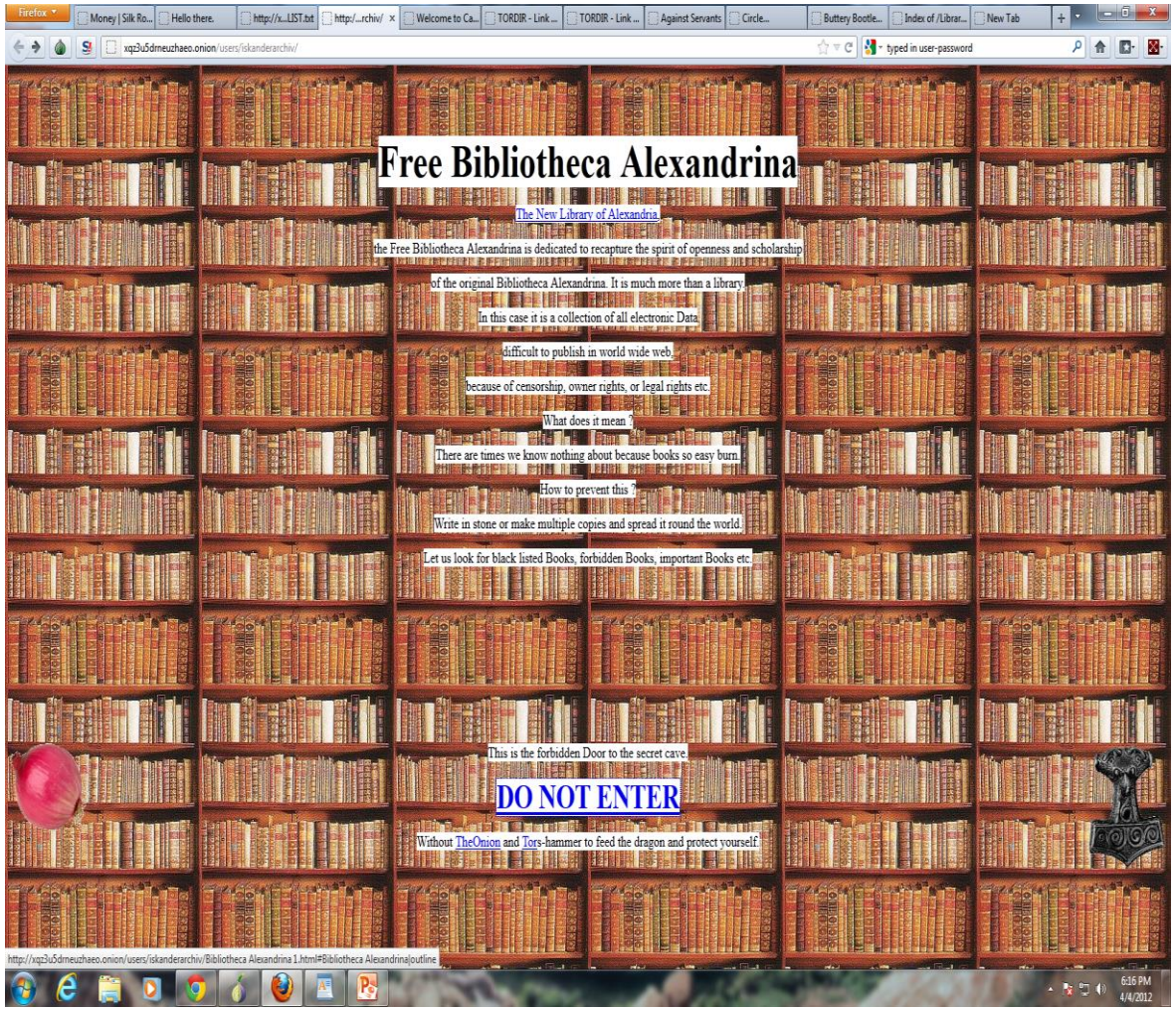
Inside (cont'd)

- 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 many different military type documents and guidebooks



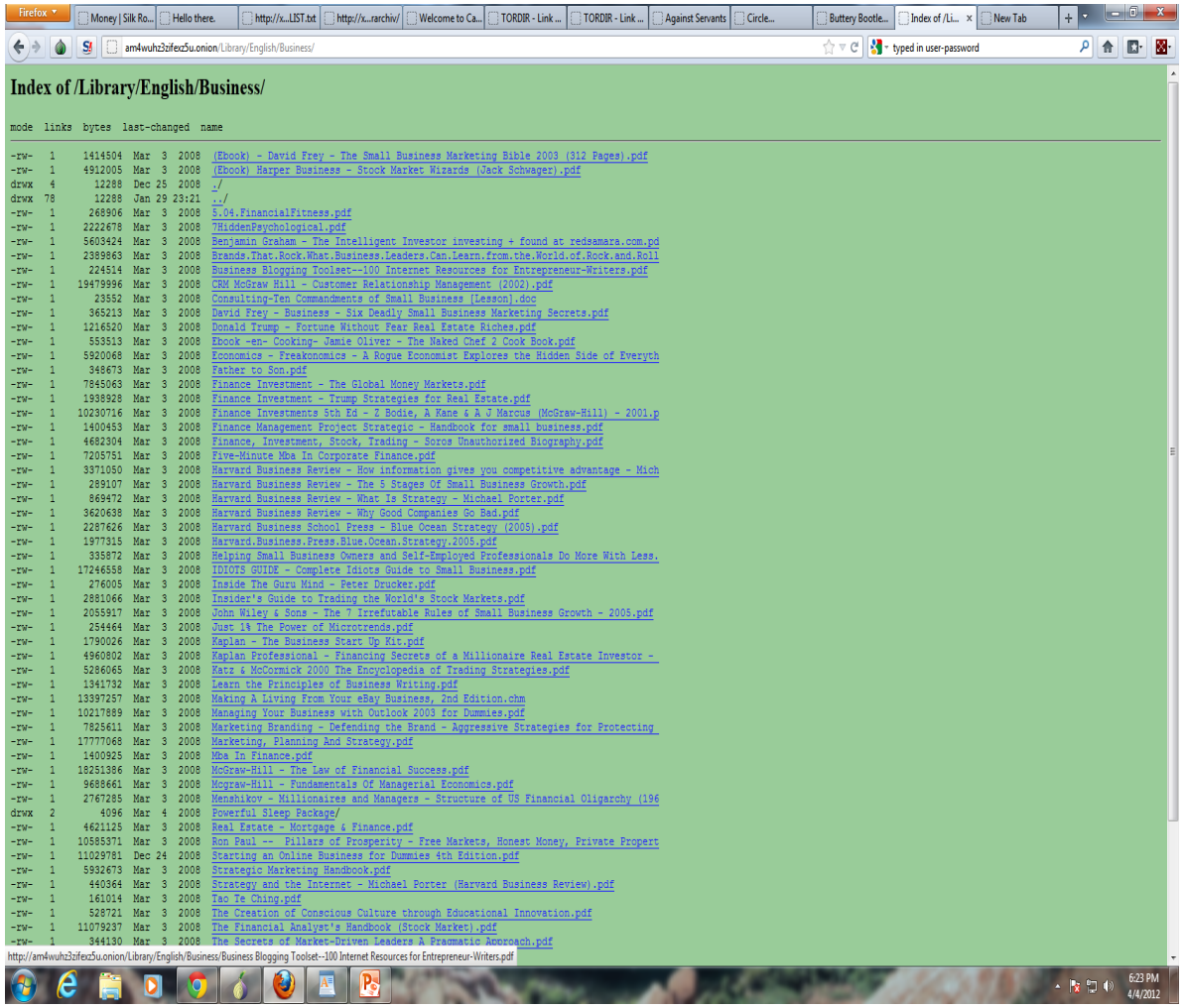
Inside (cont'd)

- 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.



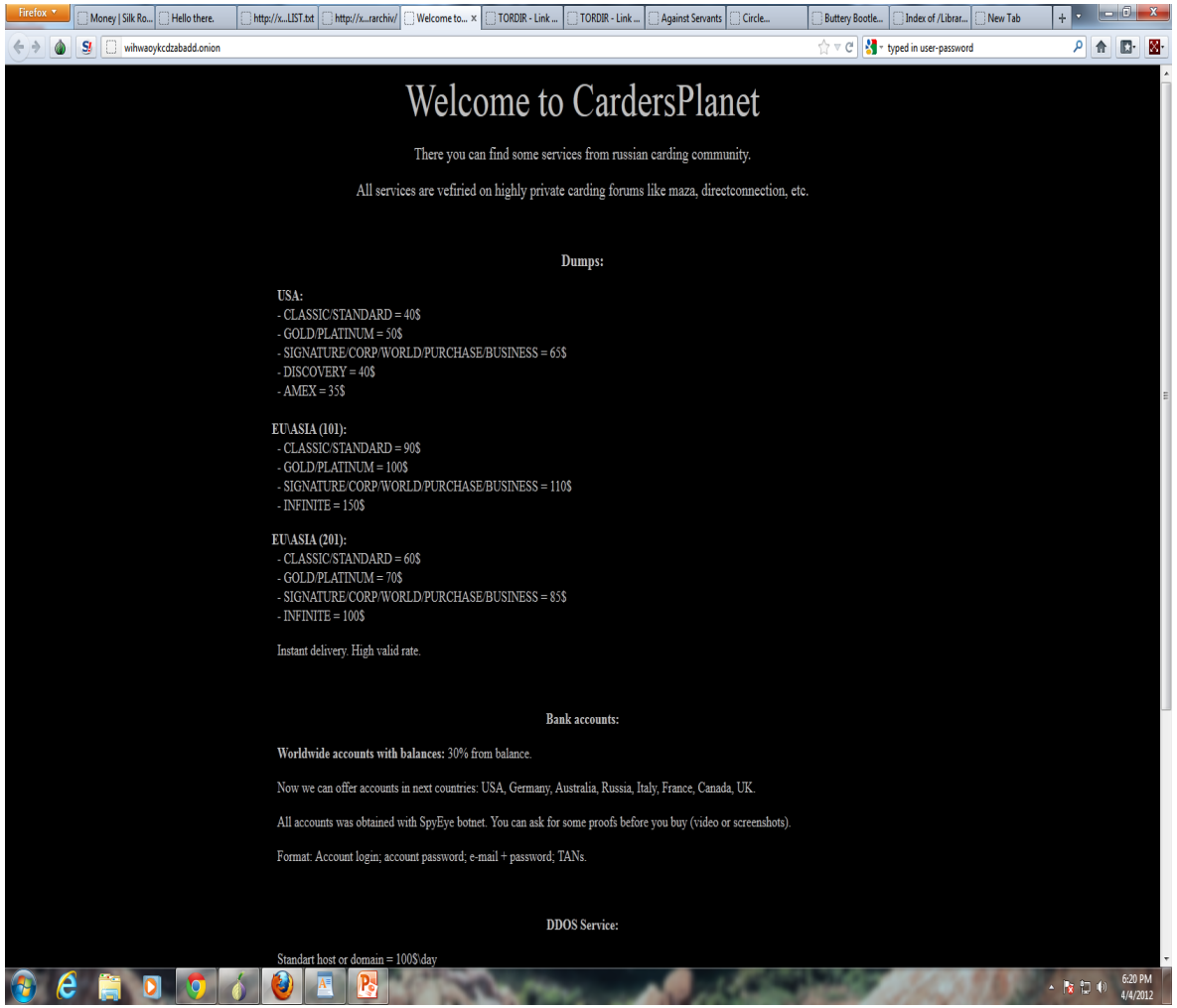
Inside (cont'd)

- 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.



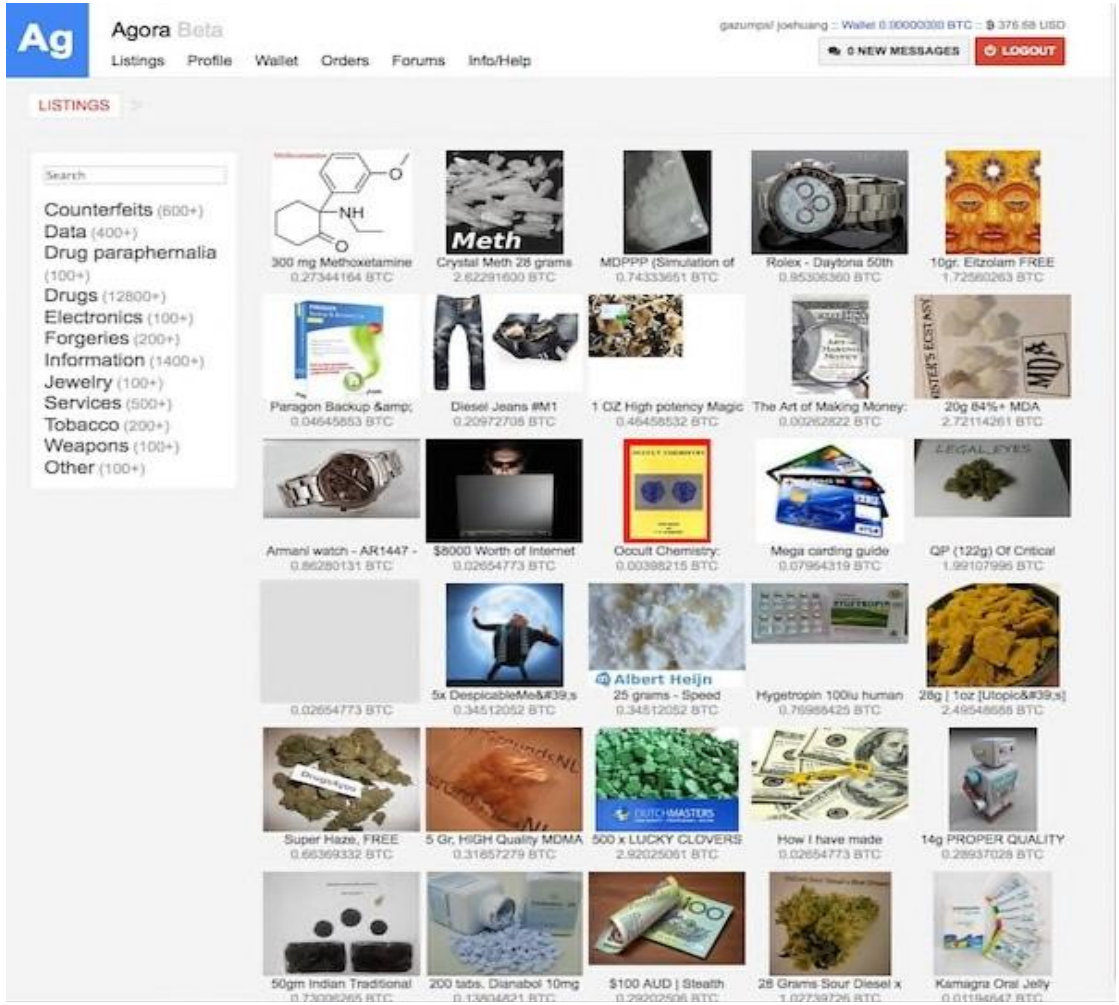
Inside (cont'd)

- 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.

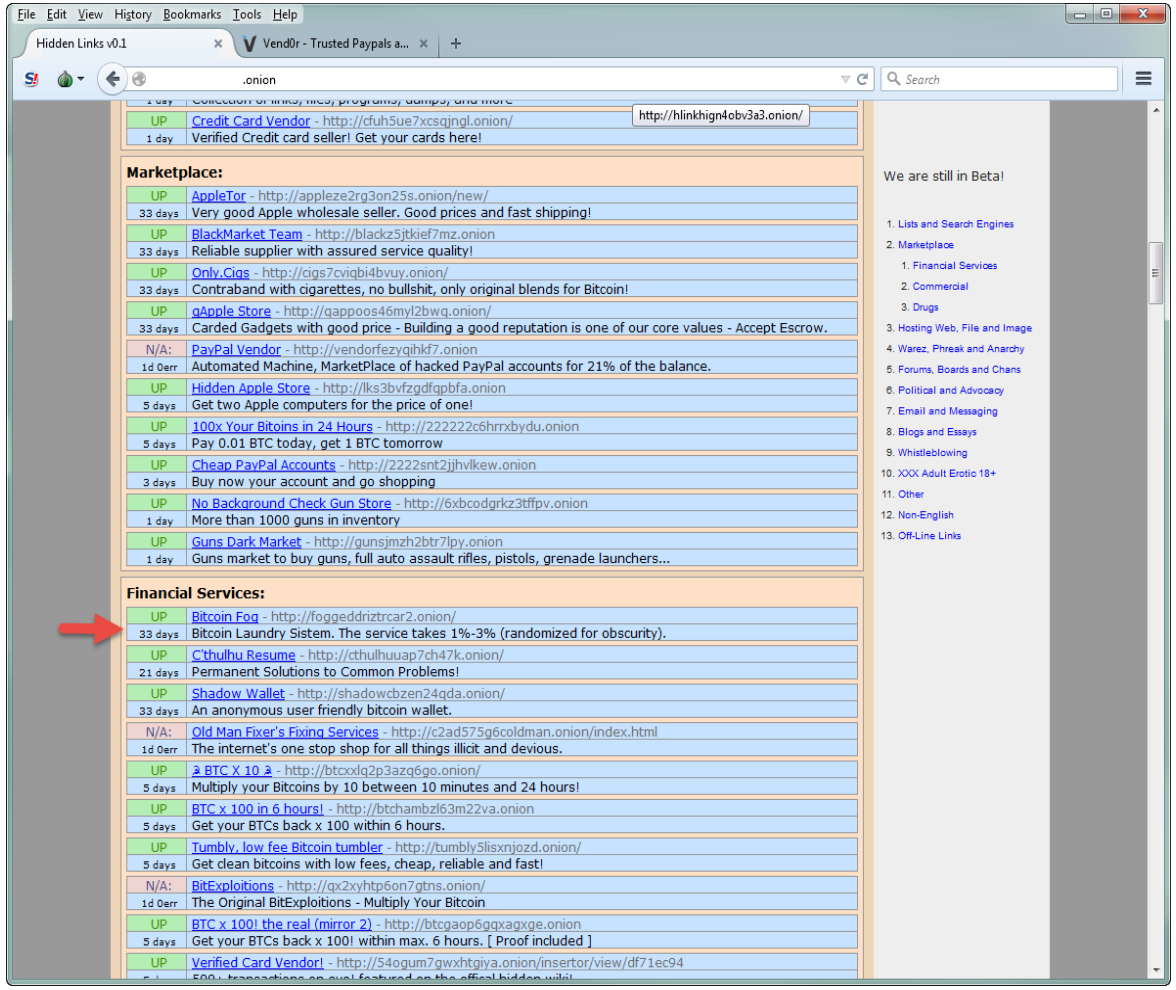


Inside (cont'd)

- Agora



- Hidden links



Inside (cont'd)

- Credit cards

File Edit View History Bookmarks Tools Help

Hidden Links v0.1 | Vend0r - Trusted Paypals a...

.onion/cards

http://vendor7zqdpty4oo.onion/cards

Vend0r | PayPal Accounts | Credit Cards New! | My Order | Cashout | Testimonials | FAQ | Support

- Cards are guaranteed to have at least $2,000 USD available balance
- **FULL REFUND or exchange for invalid/flagged/low-balance cards**
- **Cashout Guide and SOCKS Proxy, FREE with order**
- Credit Cards are sold in packs of 5, 10, and 20
- We offer packs of US or EU cards
- All cards are full dumps, including:
  - Name, Full Address, CC#, CVV, Expiration Date, DOB, IBAN (EU), SSN (US), Mother's Maiden Name, Phone, Email

US Cards		EU Cards	
5 US Cards		5 EU Cards	
Price: $50 USD (0.11948573 BTC)	Buy 5	Price: $50 USD (0.11948573 BTC)	Buy 5
10 US Cards		10 EU Cards	
Price: $90 USD (0.21507432 BTC)	Buy 10	Price: $90 USD (0.21507432 BTC)	Buy 10
20 US Cards		20 EU Cards	
Price: $170 USD (0.40625149 BTC)	Buy 20	Price: $170 USD (0.40625149 BTC)	Buy 20

- Drugs

File Edit View History Bookmarks Tools Help

Hidden Links v0.1 | Vend0r - Trusted Paypals a... | Peoples Drug Store - The D...

.onion/index.php?cat=200

http://newpdsuslmzqazvr.onion/index.php?cat=200

PEOPLES DRUG STORE
FATHER, MOTHER, BROTHER, SISTER, ALL SHOP AT PEOPLES' DRUG STORE

Login

THE PEOPLES DRUG STORE pride ourselves on offering the best quality products at competitive prices and making every effort to go above and beyond when it comes to customer satisfaction!

Choose a category by clicking on any of the following:

Heroin, Cocaine, Ecstasy, Speed, Cannabis Prescriptions, Bitcoins and Services

WANNA MAKE SOME FREE BTC??

Tell others about this shop, and earn 5% from every purchase they will make. Simply give them the following link: http://www.peoplesdrugstore.org/?ref=YOURUSERNAME (or the original http://newpdsuslmzqazvr.onion/?ref=YOURUSERNAME) Replace YOURUSERNAME with your actual username on this site and get earnings directly to your wallet.

Cocaine(85%) & Crack

People's Drug Store pride ourselves on the HIGH QUALITY of our amazing, HIGH PURITY COCAINE

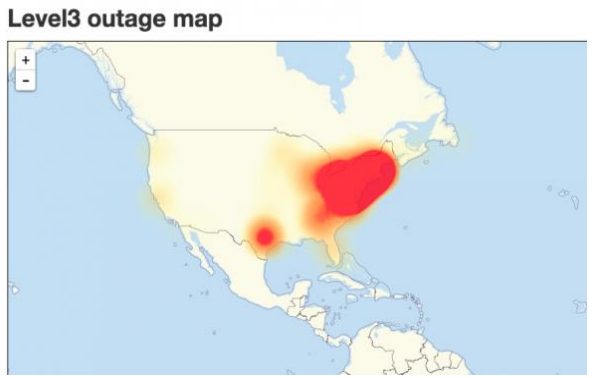
Just like our Heroin, we get our cocaine **DIRECT** from the importer (usually from Peru but sometime its from Columbia) and we always get our product given to us right off of the kilogram bricks as they come in so we can be **ABSOLUTELY POSITIVE that it was not cut or stepped on locally in any way!!**

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 human-to-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

- **IoT Attacks**



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.

Security Requirement

- Secure Booting
- Access Control
- Anti-DDoS
- Device Authentication
- Secure Software Updates and Patches

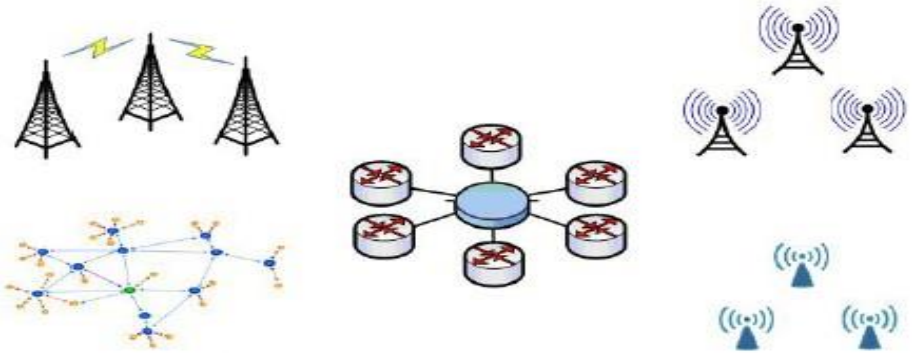
4 Layers Model of IoT

- Layers

Integrated Application

Information Processing

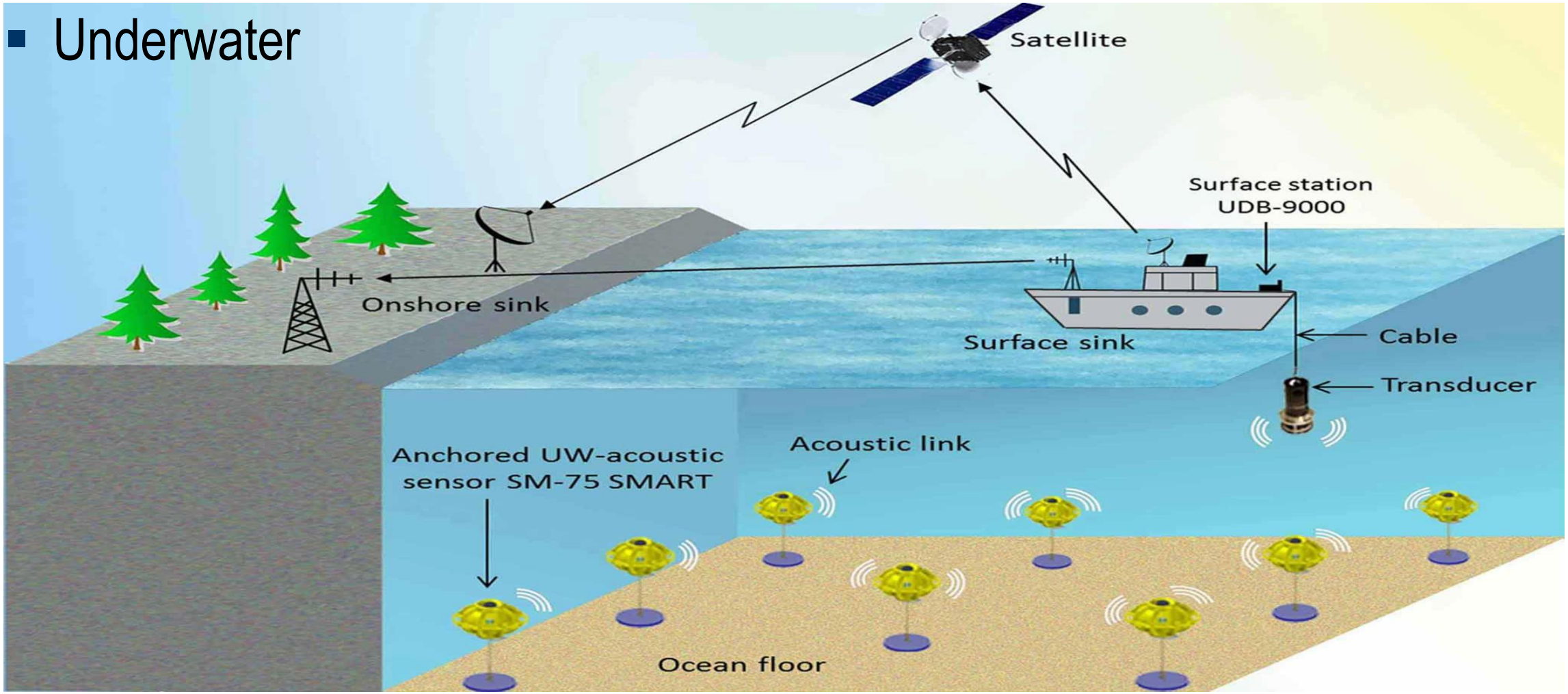
Network Construction



Sensing and Identification

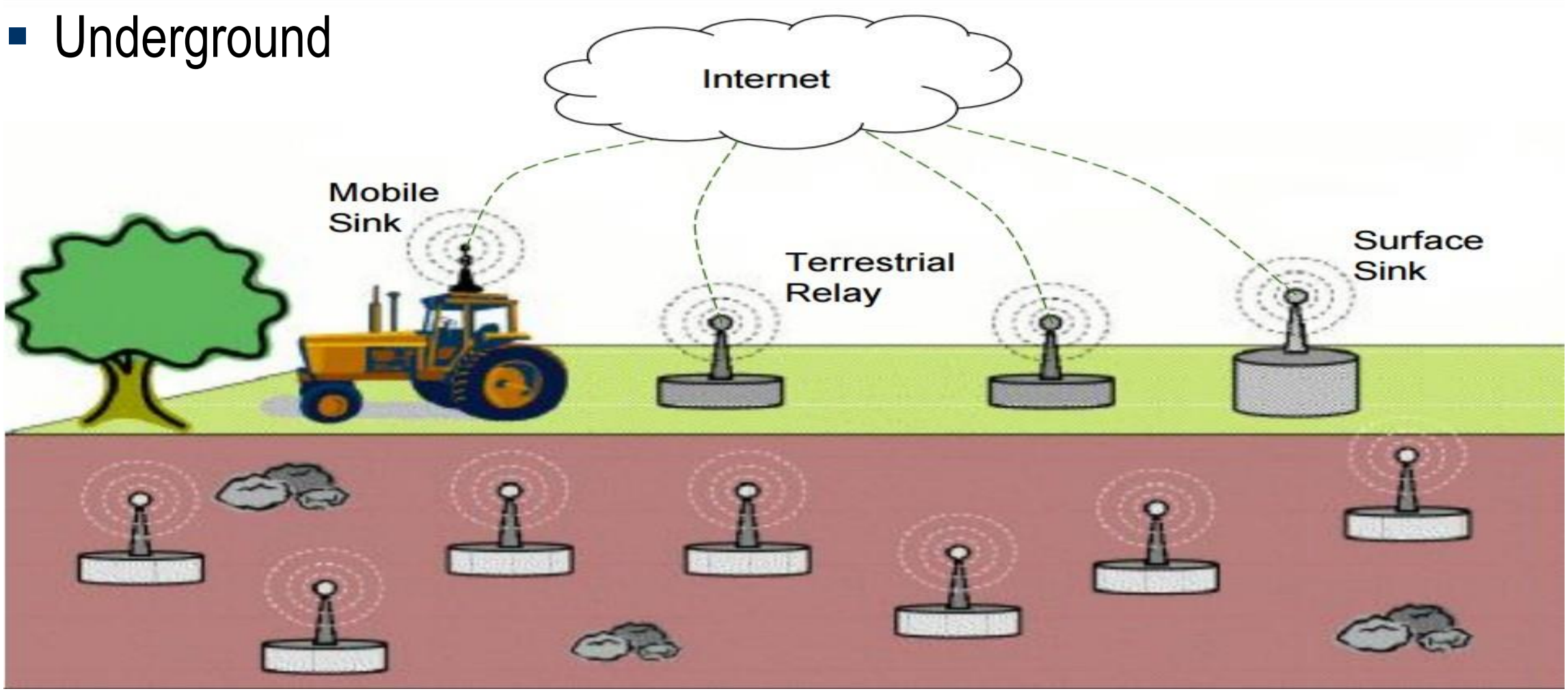
Internet of Underwater Things

- Underwater

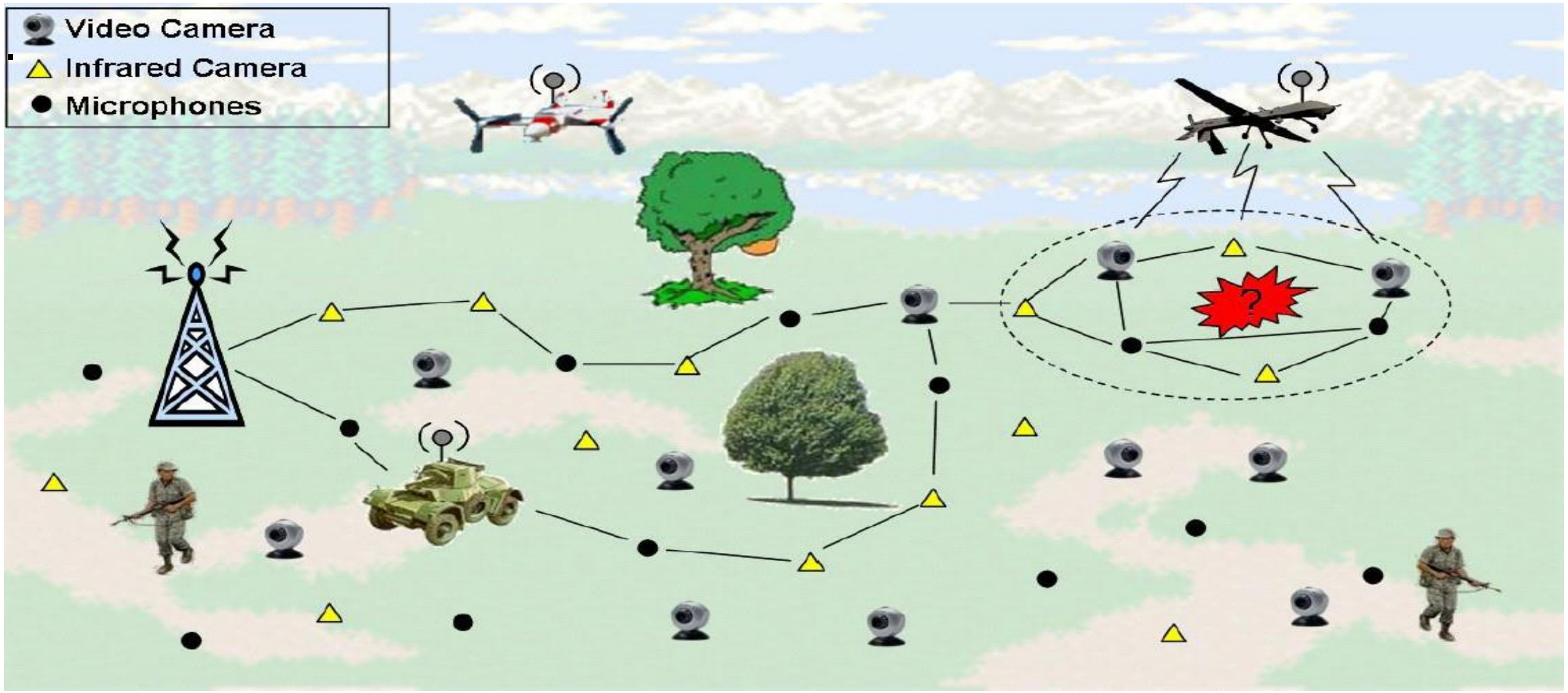


Internet of Underground Things

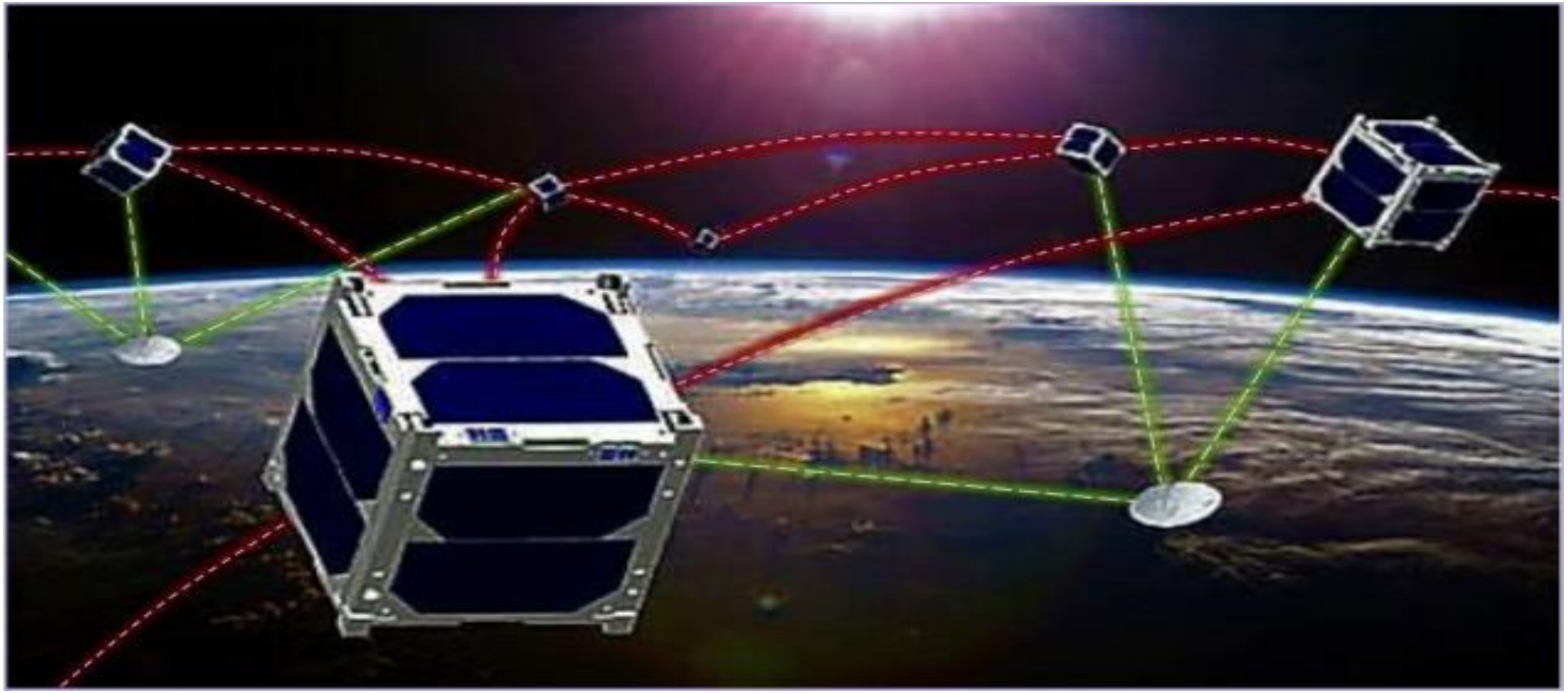
- Underground



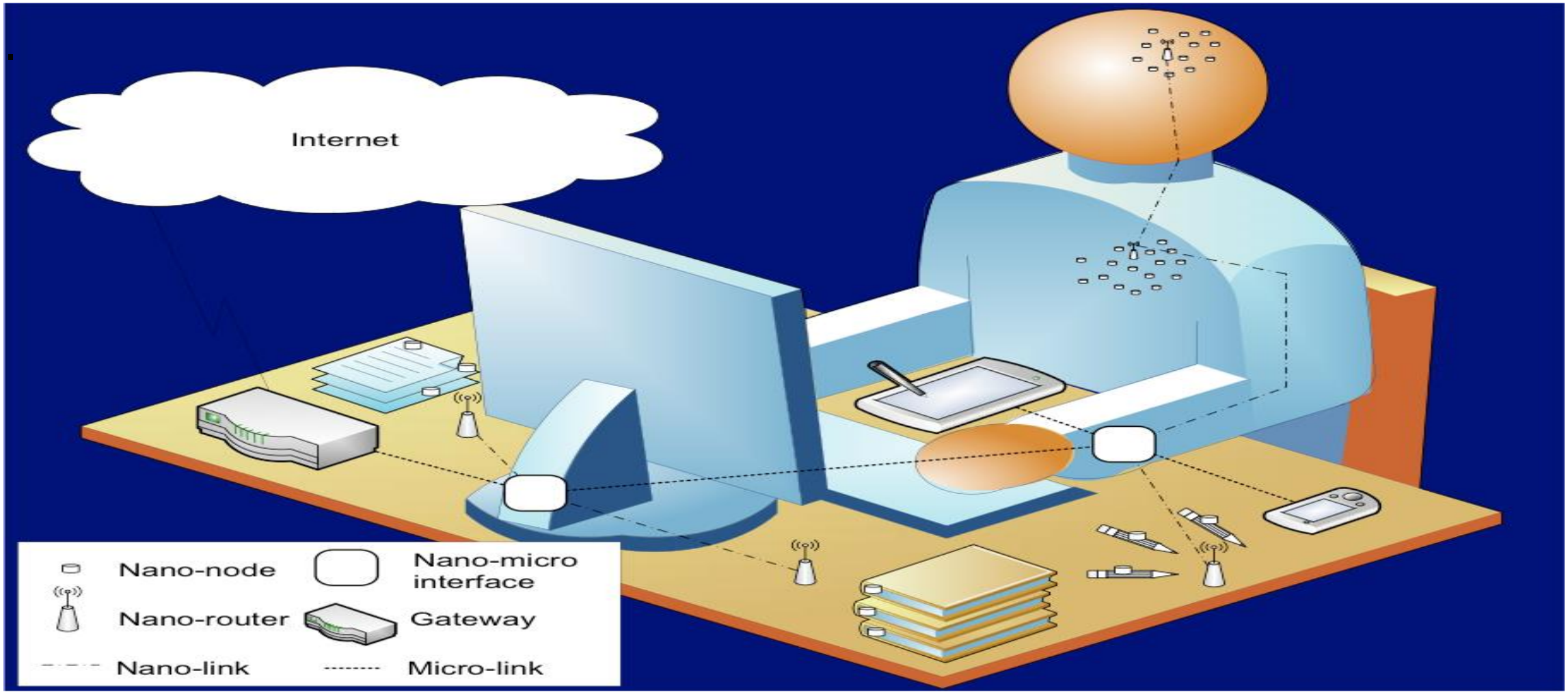
Internet of Battlefield Things



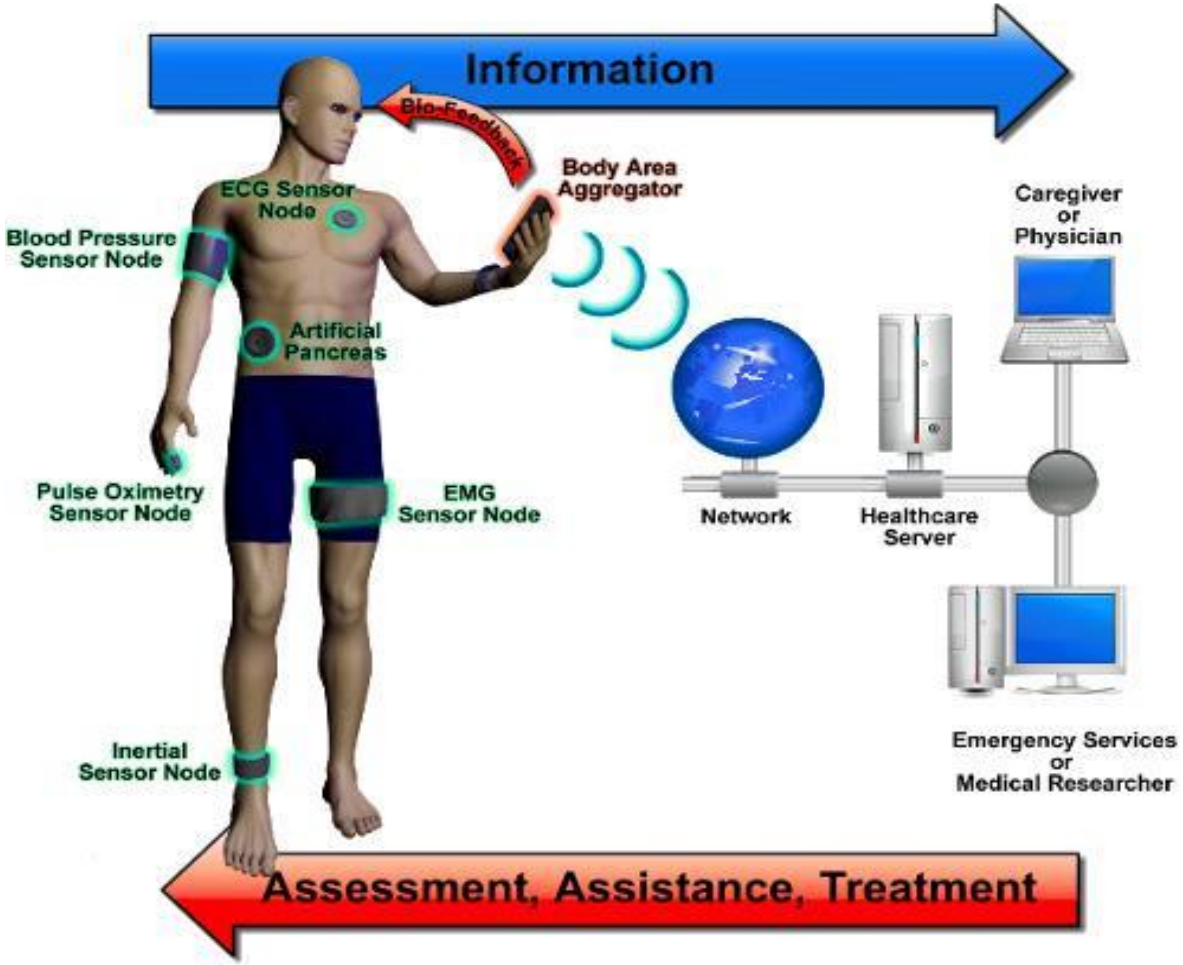
Internet of Space Things



Internet of Nanothings



Internet of Bio-Nanothings



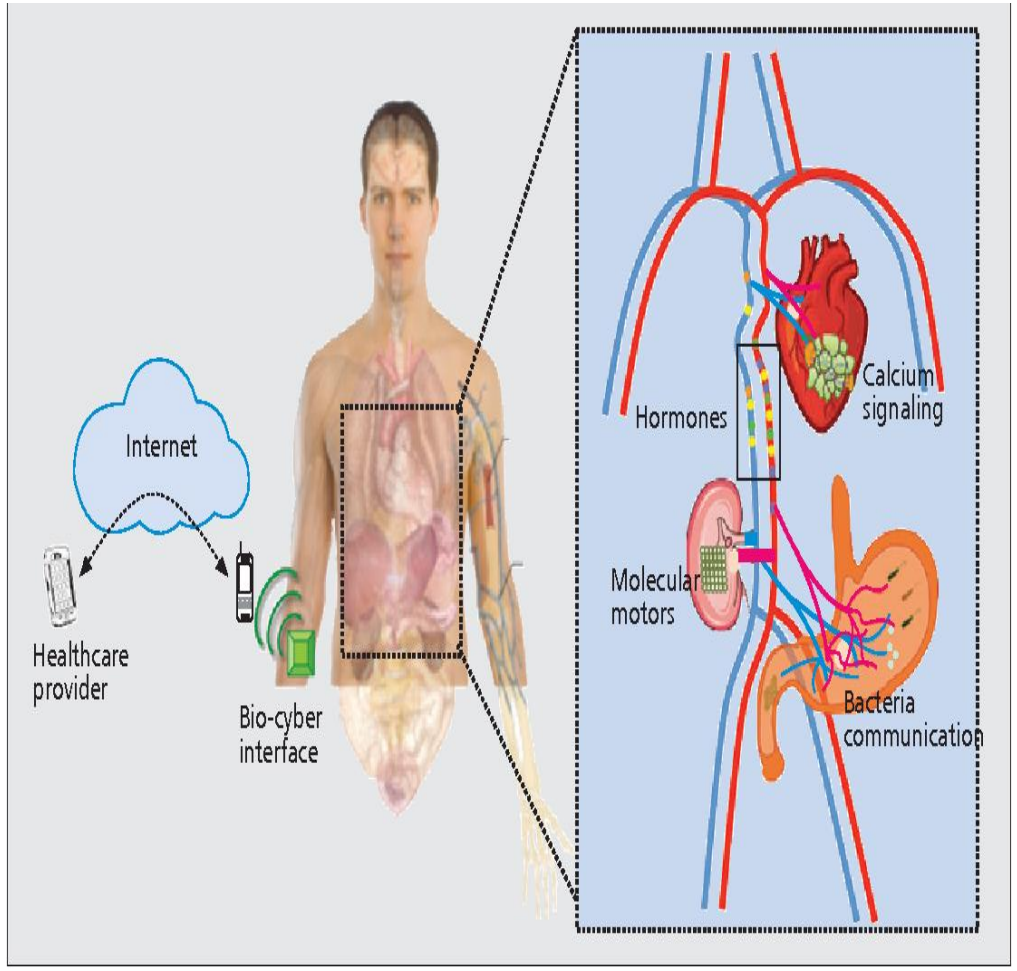


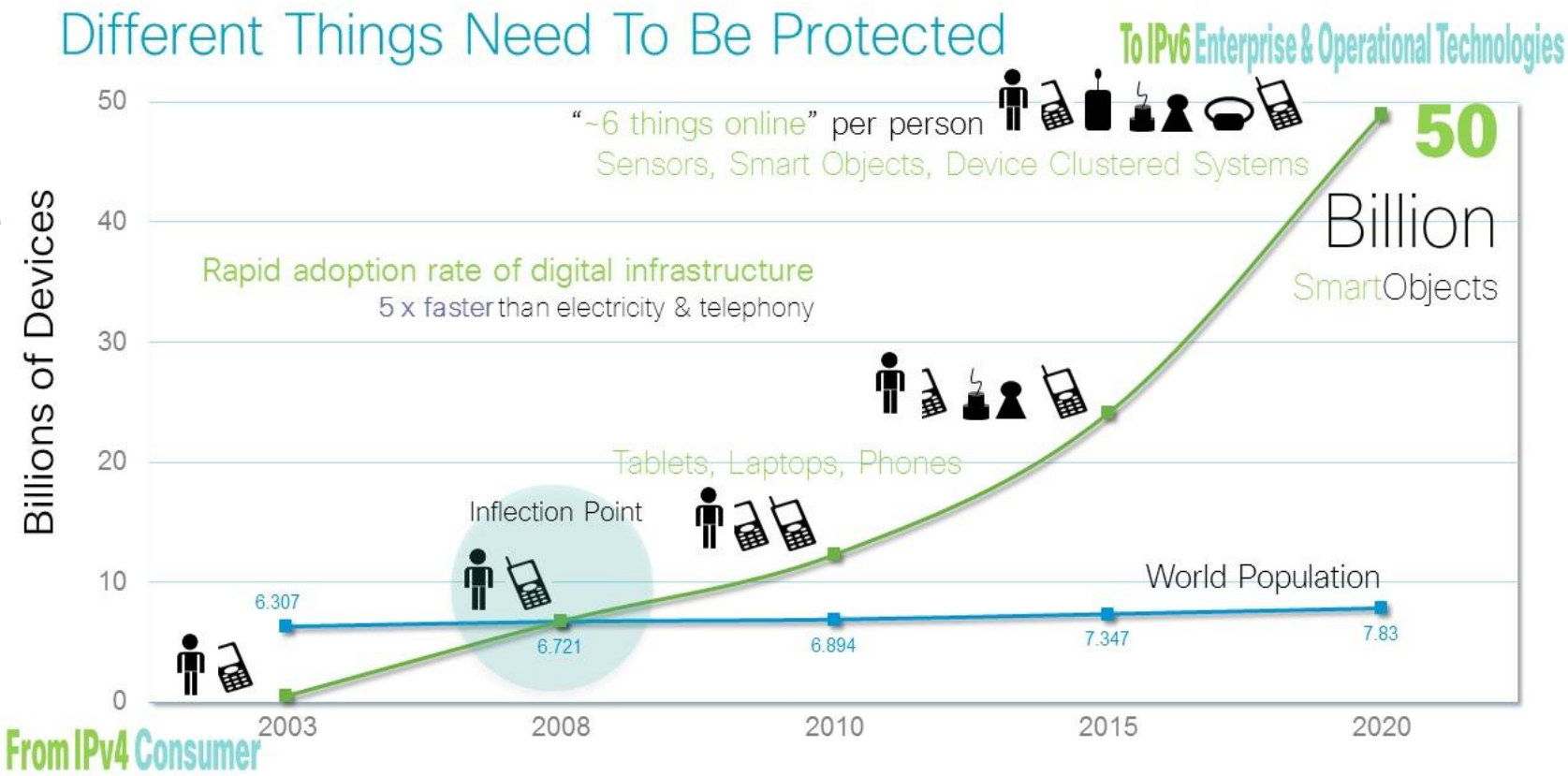
Figure 4. Network architecture for the Internet of Bio-NanoThings for Intra-body applications.

Internet of Things: Perspectives

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

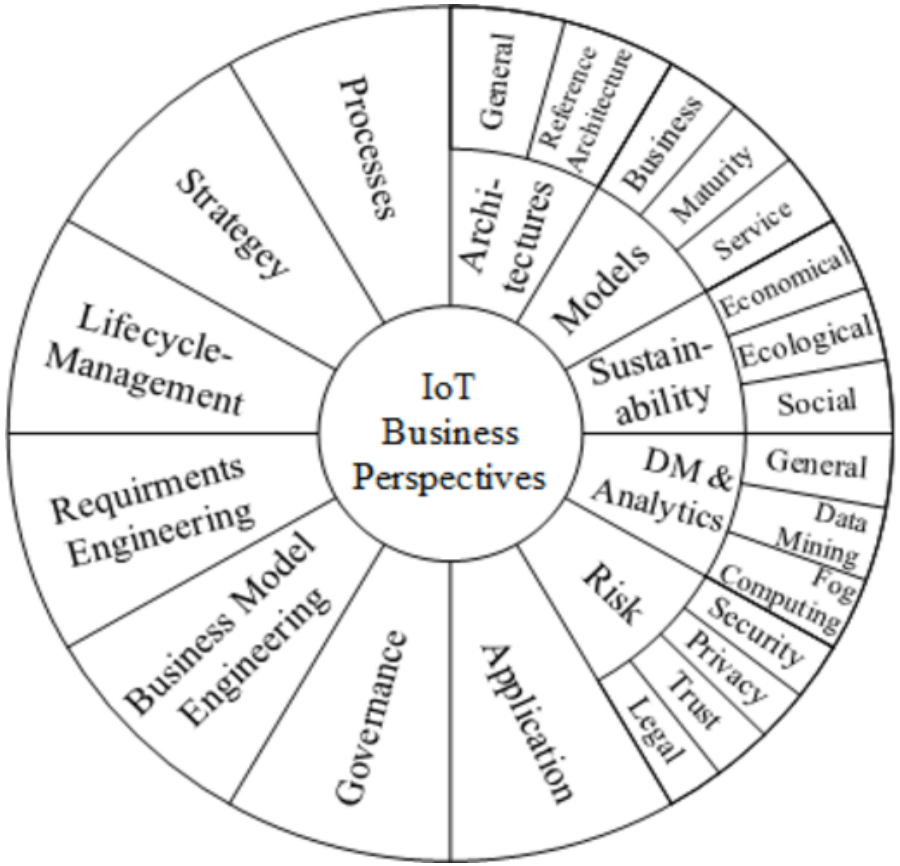
- Outdoors
- Indoors
- On the Move

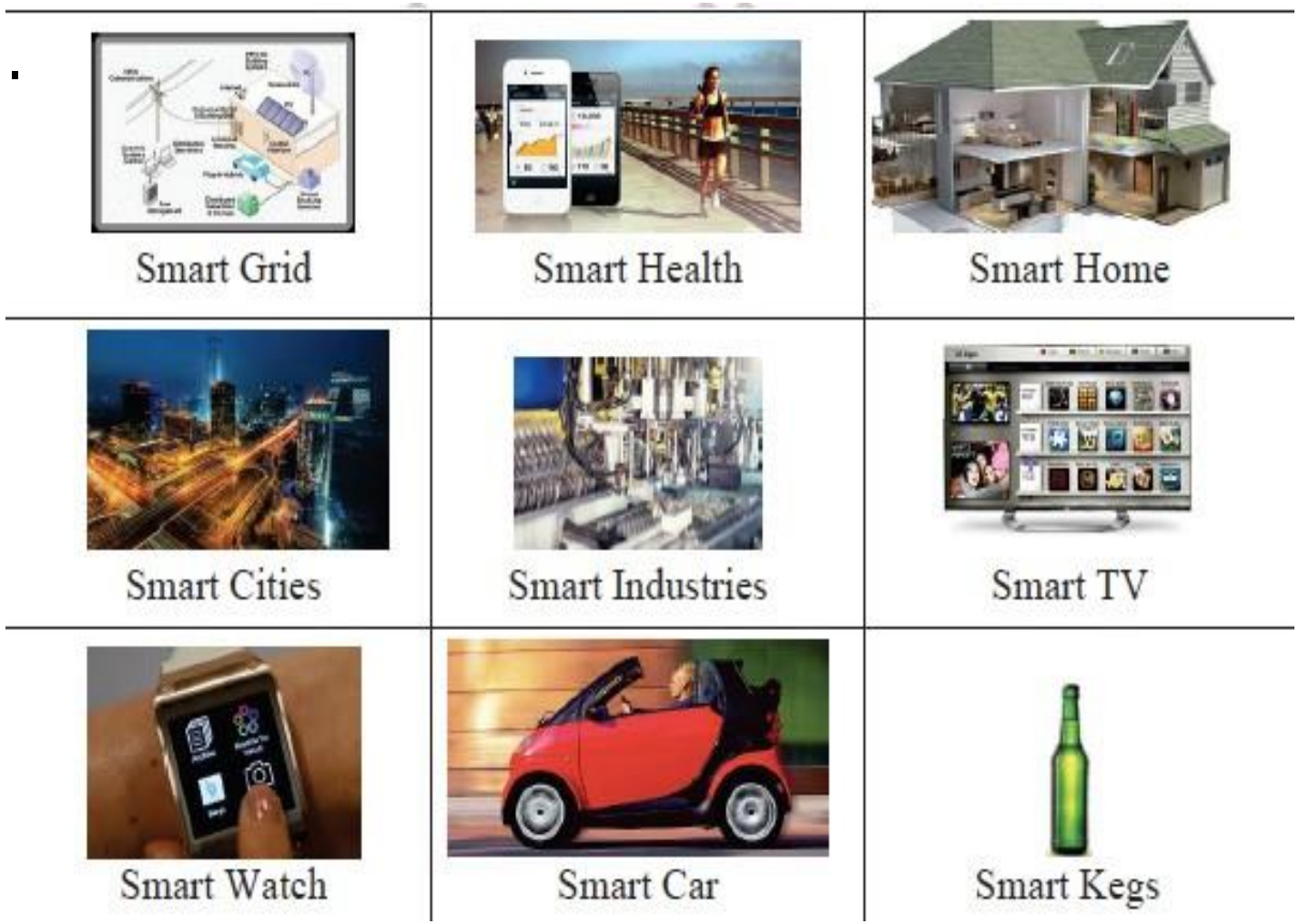
- Human to Human (H2H)
- Human to Thing (H2T)
- Thing to Thing (T2T)



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

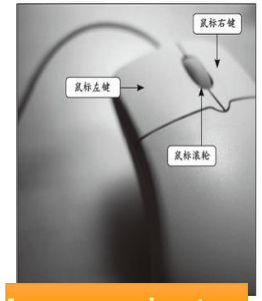
USB Key

SMS Code

OneKey Confirmation

OTP Token

Keyboard Pressing

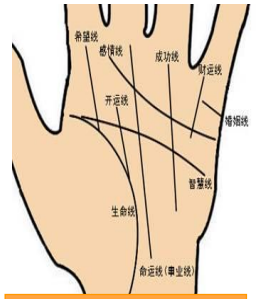


Mouse moving track

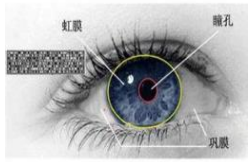
Handwriting

Finger Pressing

Fingerprint



Palmprint



Iris

Face

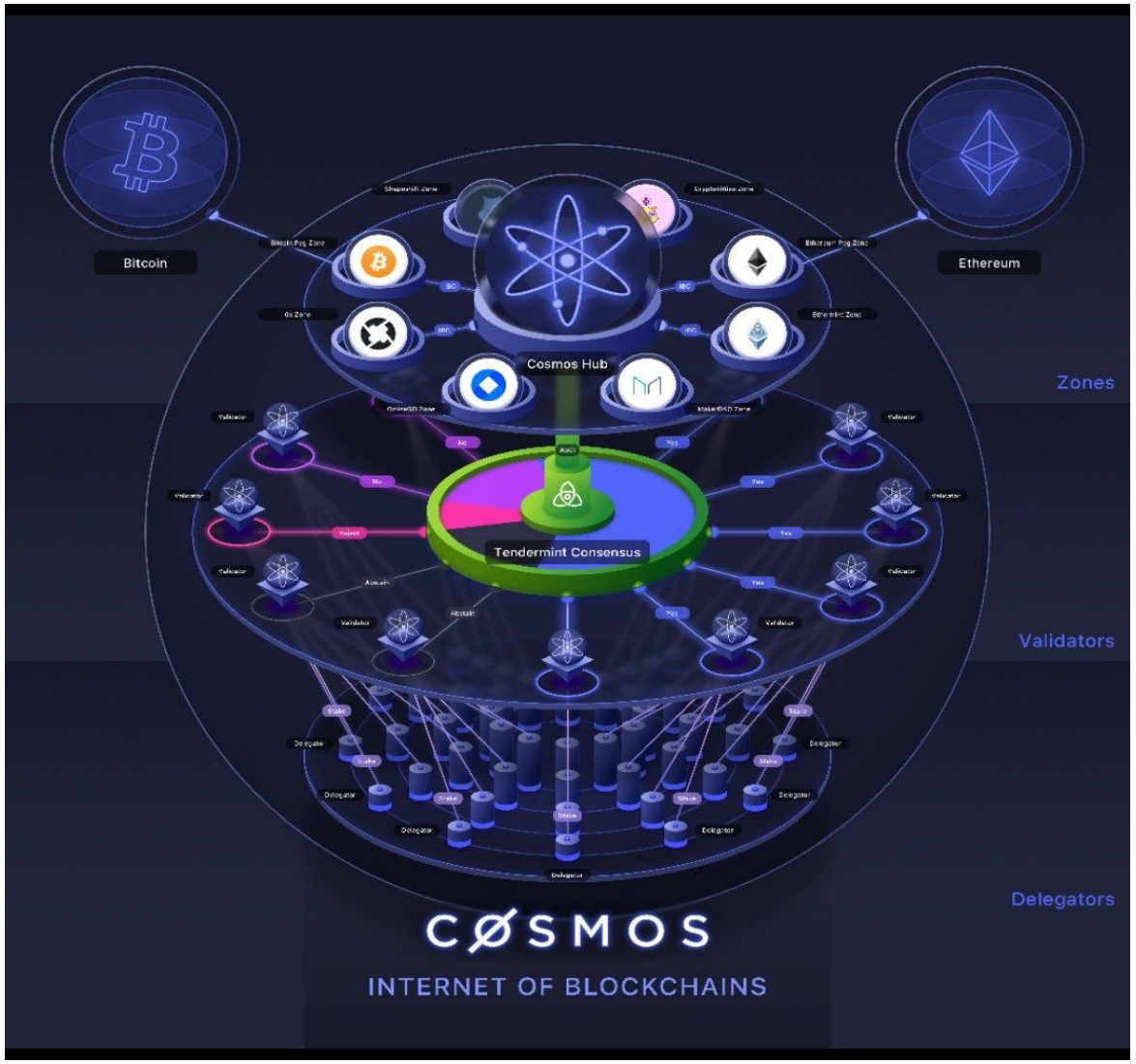
Web API for “Human ontology authentication” ?

Advantages

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

The Internet of Blockchain +++

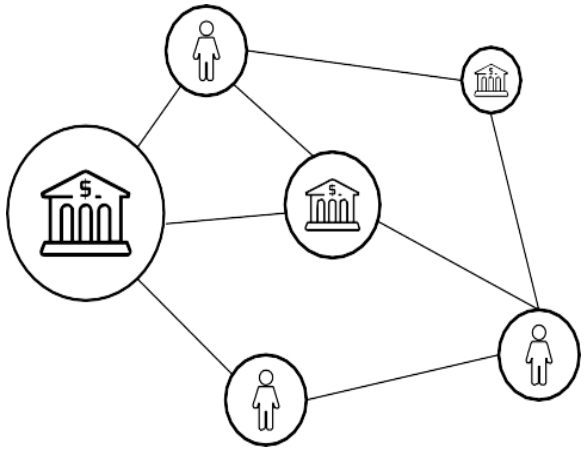
- Inter Blockchain Communication (IBC):The Cosmos Network has the Inter Blockchain Communication (IBC) protocol to allow blockchains to interact with other blockchains. The network of blockchains will communicate through IBC, with the Cosmos Network as the central hub. Blockchains are connected in a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



- https://medium.com/@davekaj/blockchain-interoperability-cosmos-vs-polkadot-48097d54d2e2

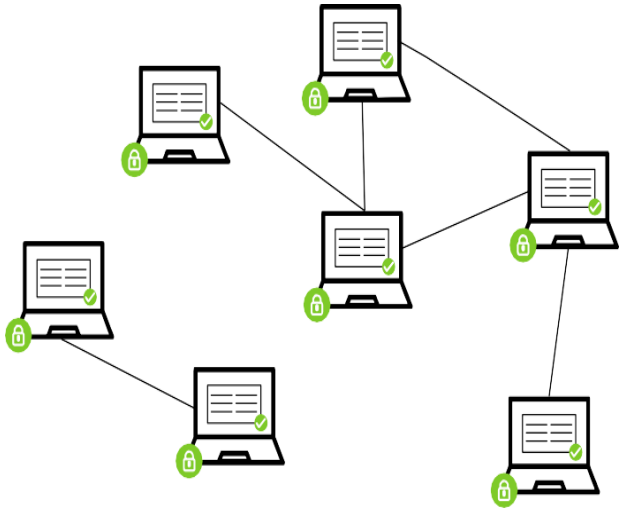
Block Chain in Brief

- Current Financial System



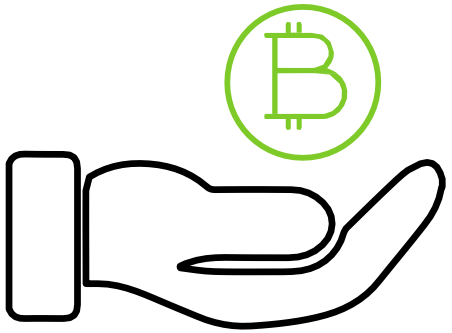
- Central authorities (bank, fed, notary, escrow, etc.) transfer actual value between two parties.
- Multiple intermediaries and record-keeping are required to facilitate transfer of assets and create trust

- 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-and-mortar 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.

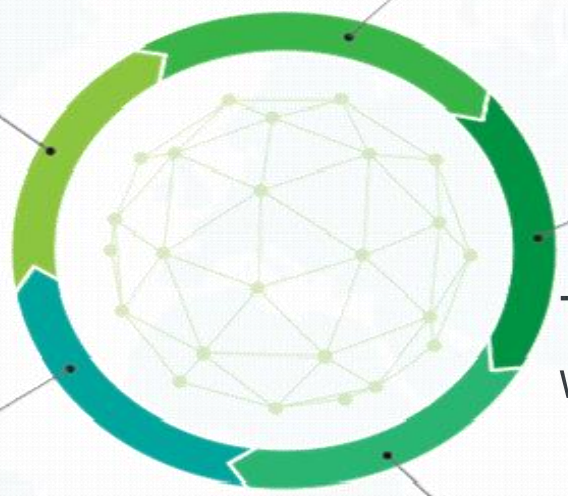
- Distributed
- Secure
- Log file

Blockchain (cont'd)

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

Every **viable transaction** is stored in the **shared public ledger**

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



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

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

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

Blockchain (cont'd)

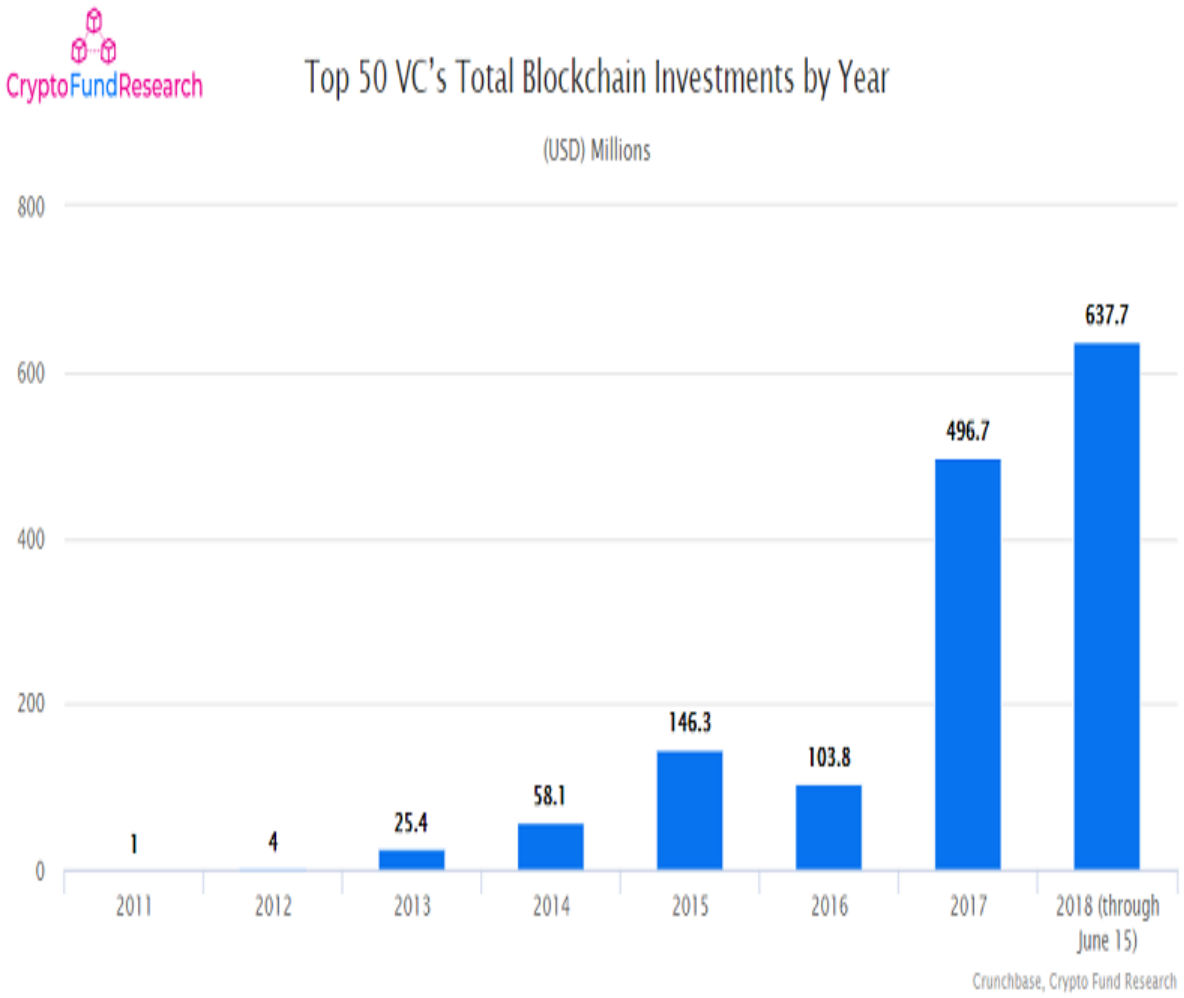
- BlockChains are essentially facilitated on a platform of distributed databases with some inbuilt pre-agreed technical and business logic criteria, kept in sync via peer-to-peer mechanisms and pre-agreed consensus algorithms. These are the BlockChain Ledgers.
- Data stored on BlockChains are considered 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	Windows Azure, ethereum, factom, Digital Asset Holdings, eris INDUSTRIES, chain, Blockstream, bloq, CREDITS, Blockstack.io, Counterparty, BLOCKCYPHER, symbiont, consensys
WALLETS	xapo, trucoin, coinbase, BitGo, Gem, ARMORY, BLOCKCHAIN, CIRCLE
IDENTITY	onename,
ASSET TRADING	Serica, Voatz, clearmatics, everledger
EXCHANGES	CIRCLE, coinsetter, BITSTAMP, coinx, itBit, kraken
PAYMENT PROCESSORS	Bitnet, bitpay, GOCOIN, coinbase
LOYALITY & GIFT CARDS	loyyal, gyft
HARDWARE	BitFury, KnCMiner, Storj.io
PAYMENTS & REMITTANCES	ripple, CIRCLE, REBIT, stellar, Bitspark, ABRA
CONSORTIA, VCs & ORGANIZATIONS	R3, HYPERLEDGER PROJECT, coala, DIGITAL CURRENCY GROUP

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

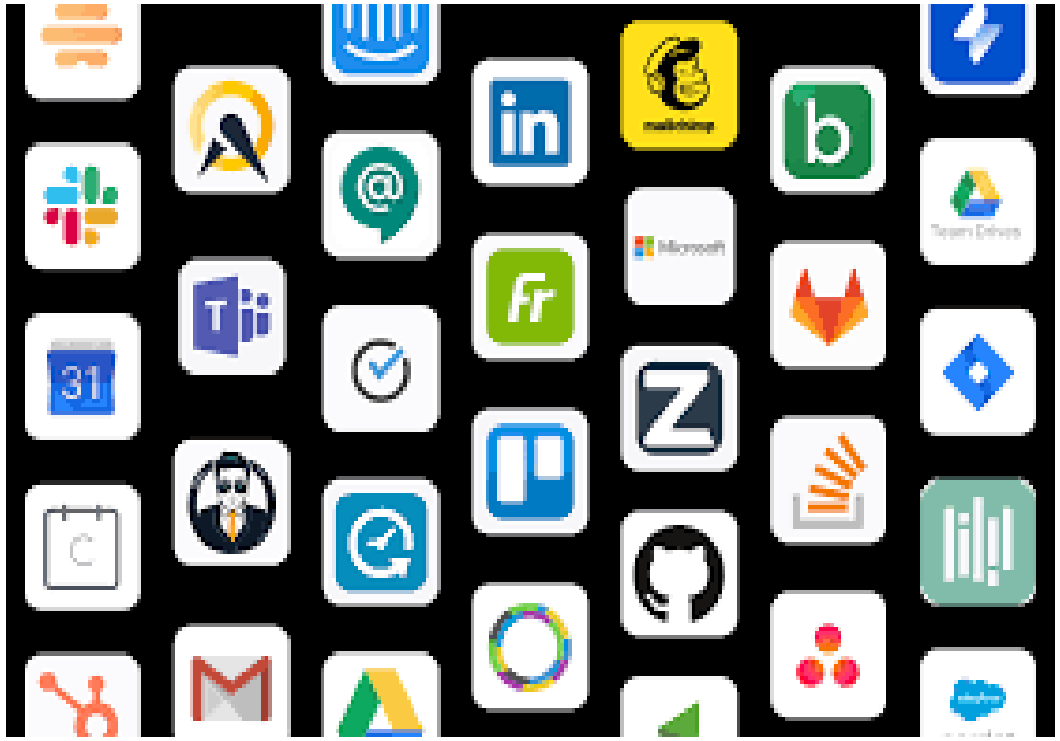
Go to the virtual room, and complete the activity thread.

3) Fifth Lab

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.



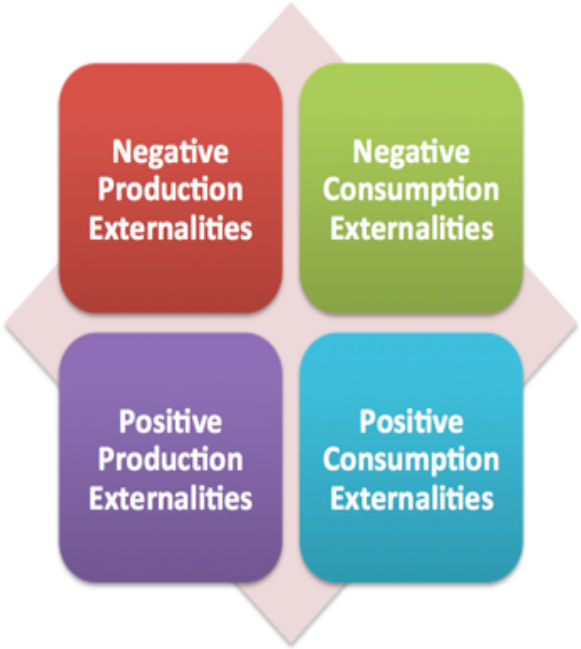
Market Externalities

- 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

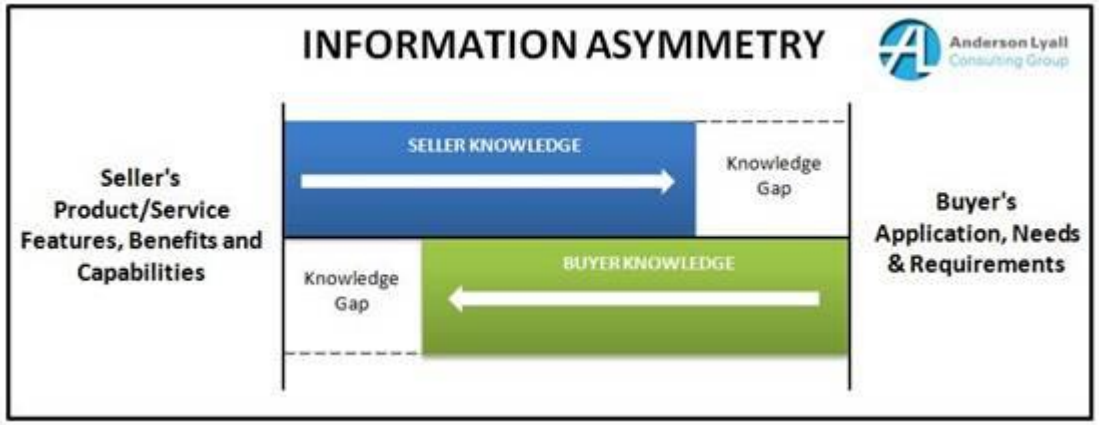
Externalities are a major cause of market failure and occur in nearly every market – be clear on effects for producers and consumers

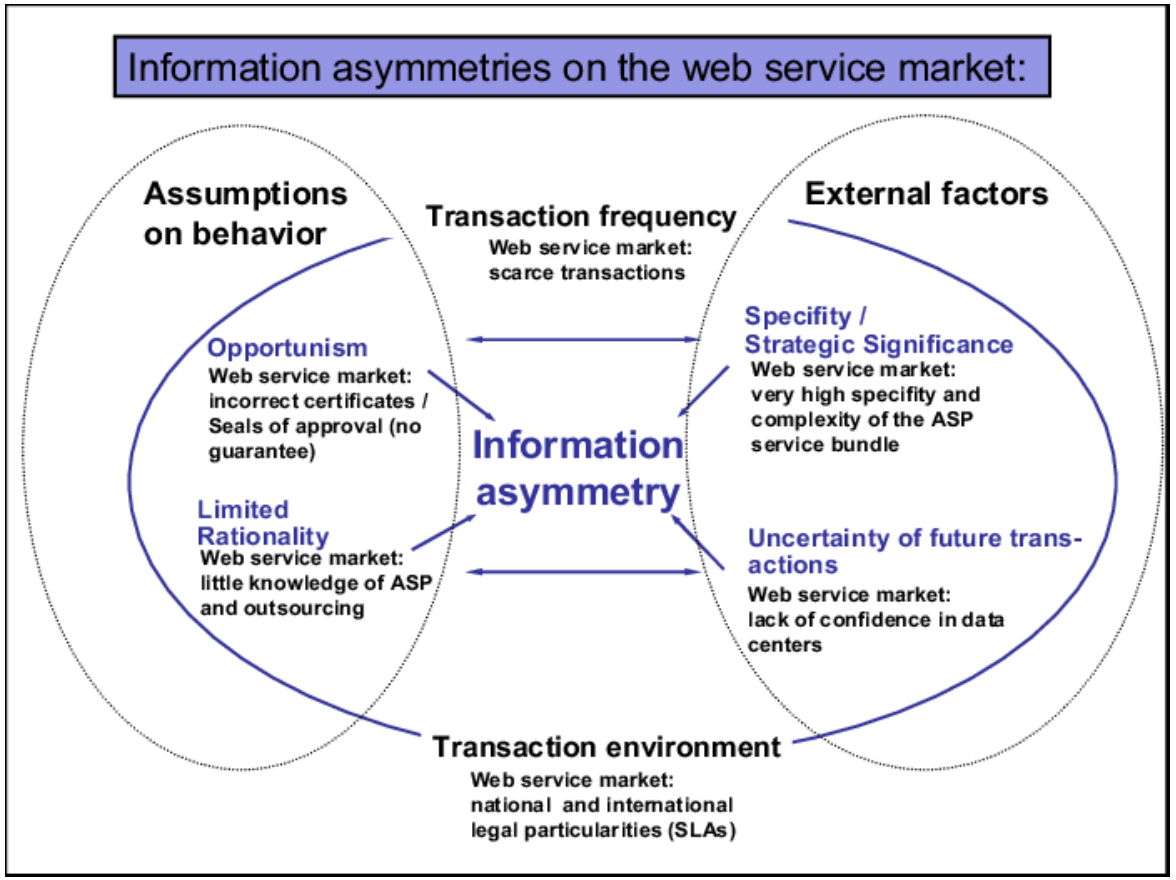
- Externalities are **spill-over effects** arising from production and consumption for which no appropriate compensation is paid
- Externalities lie **outside the market transaction**
- Externalities cause **market failure** if the **price mechanism** does not take account of the **social costs** and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



Market Information asymmetries

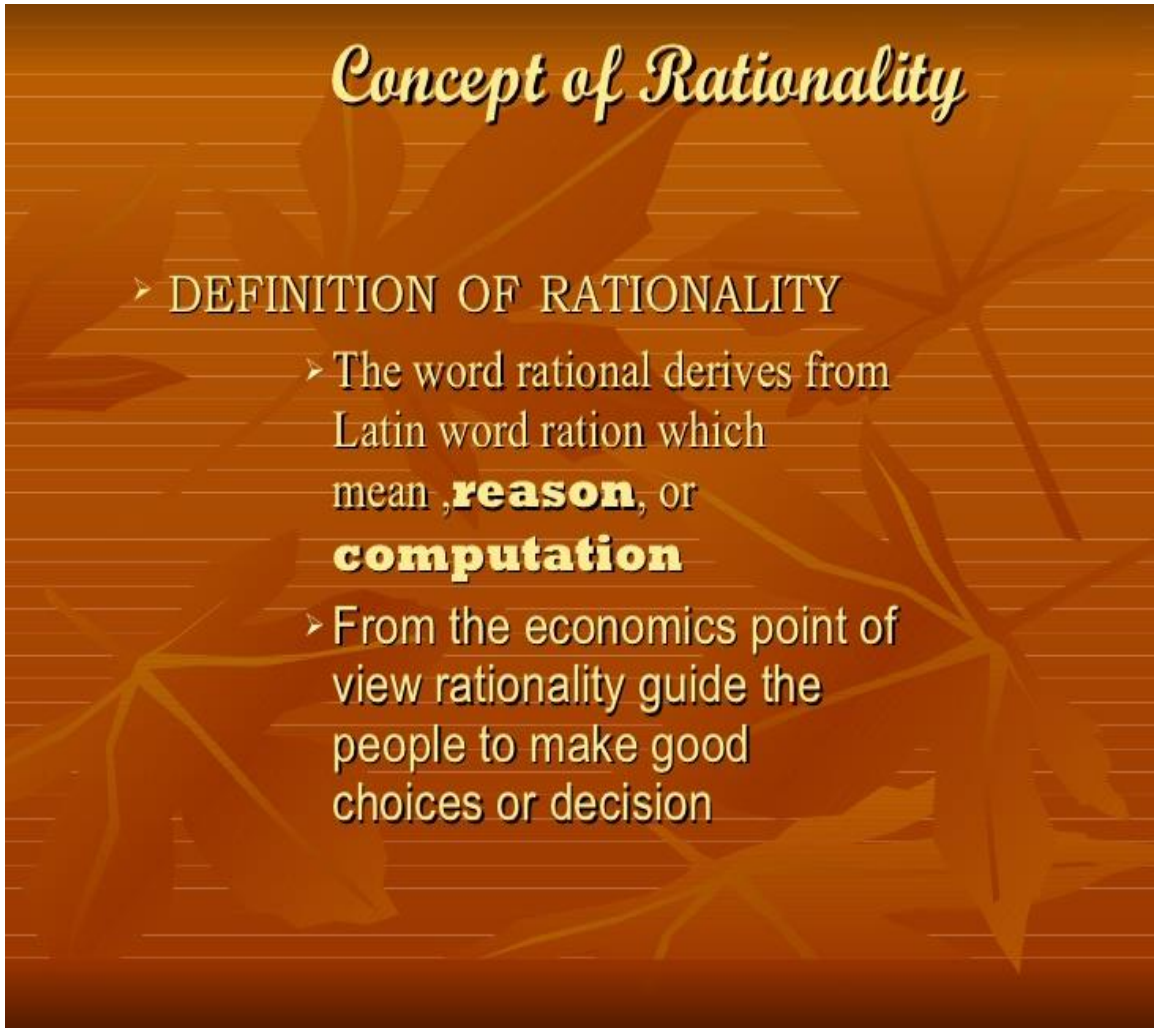
- One actor has information that another actor doesn't have, giving that first actor an advantage





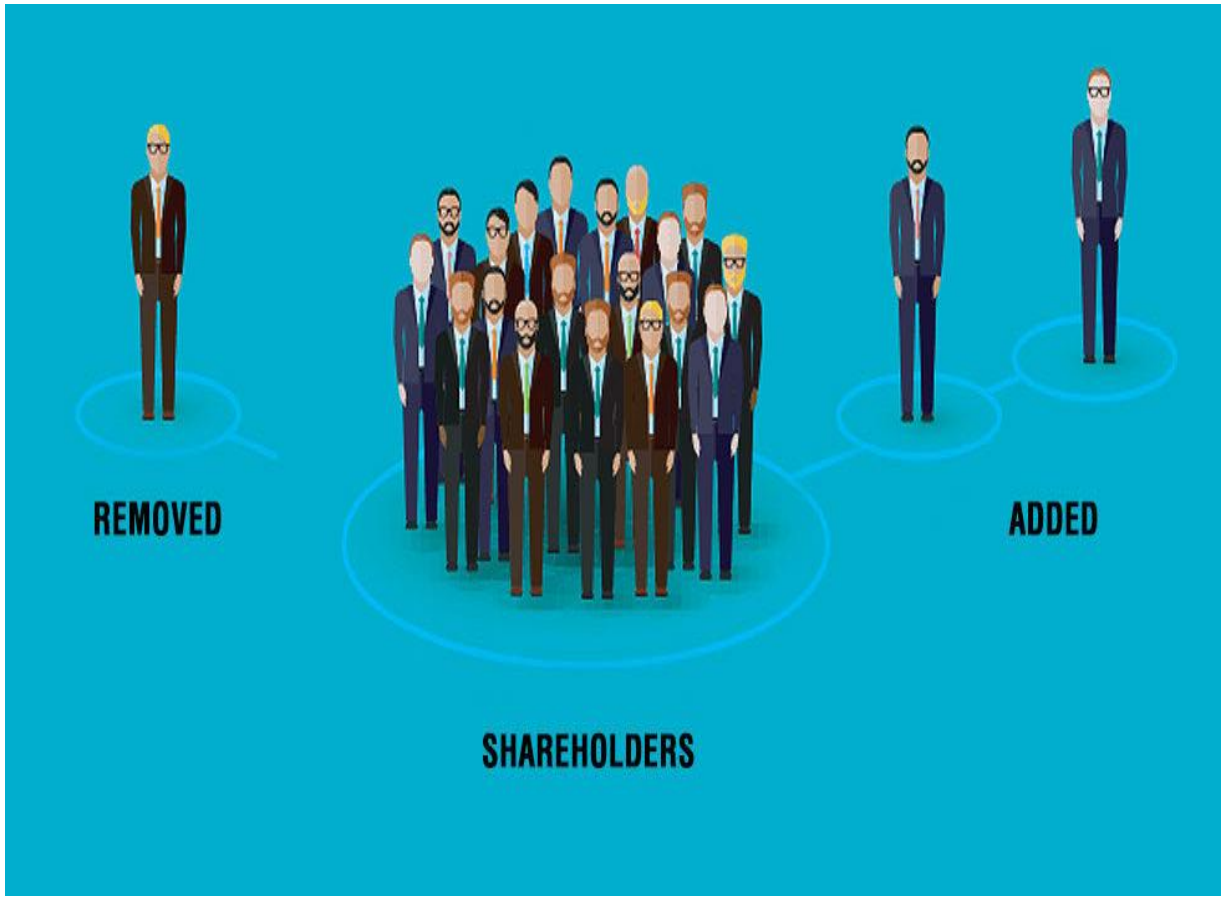
Rationality

- 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?



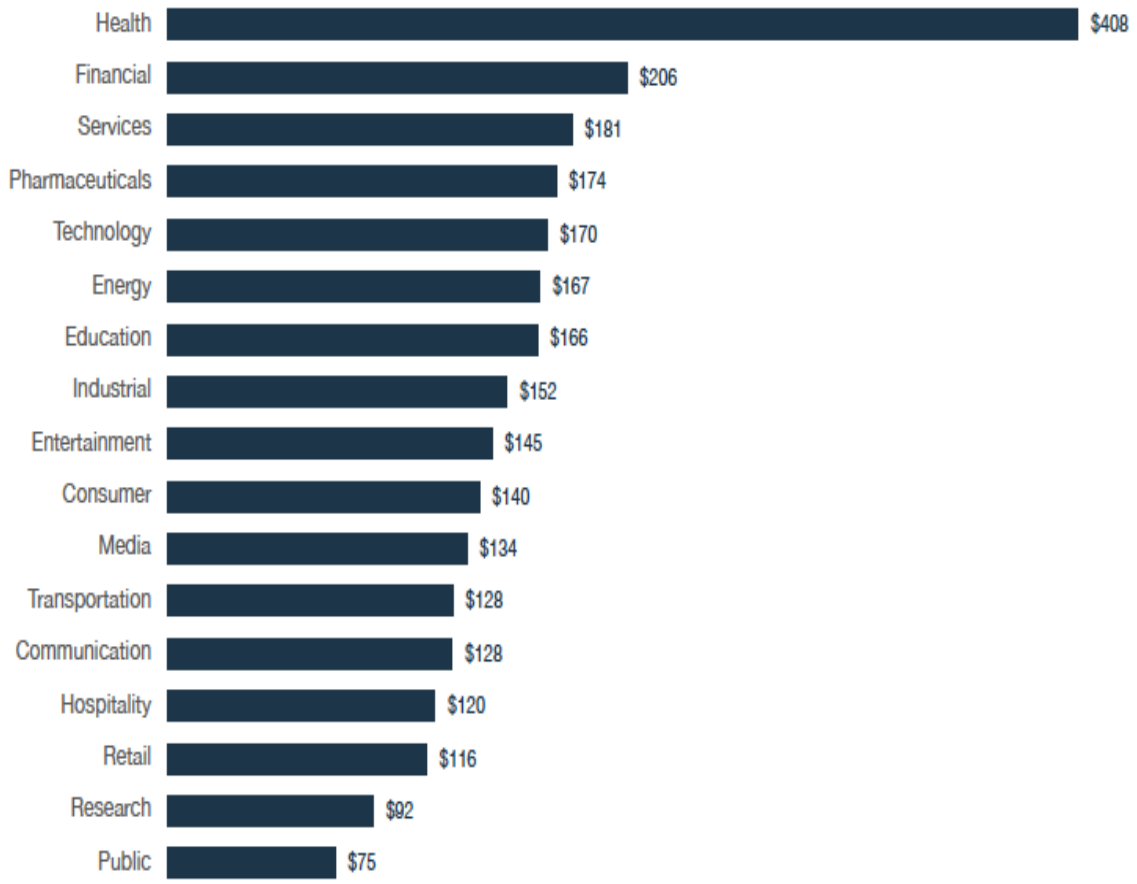
Maximizing shareholder value

- 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: https://www.ibm.com/security/data-breach



Critical moments in security

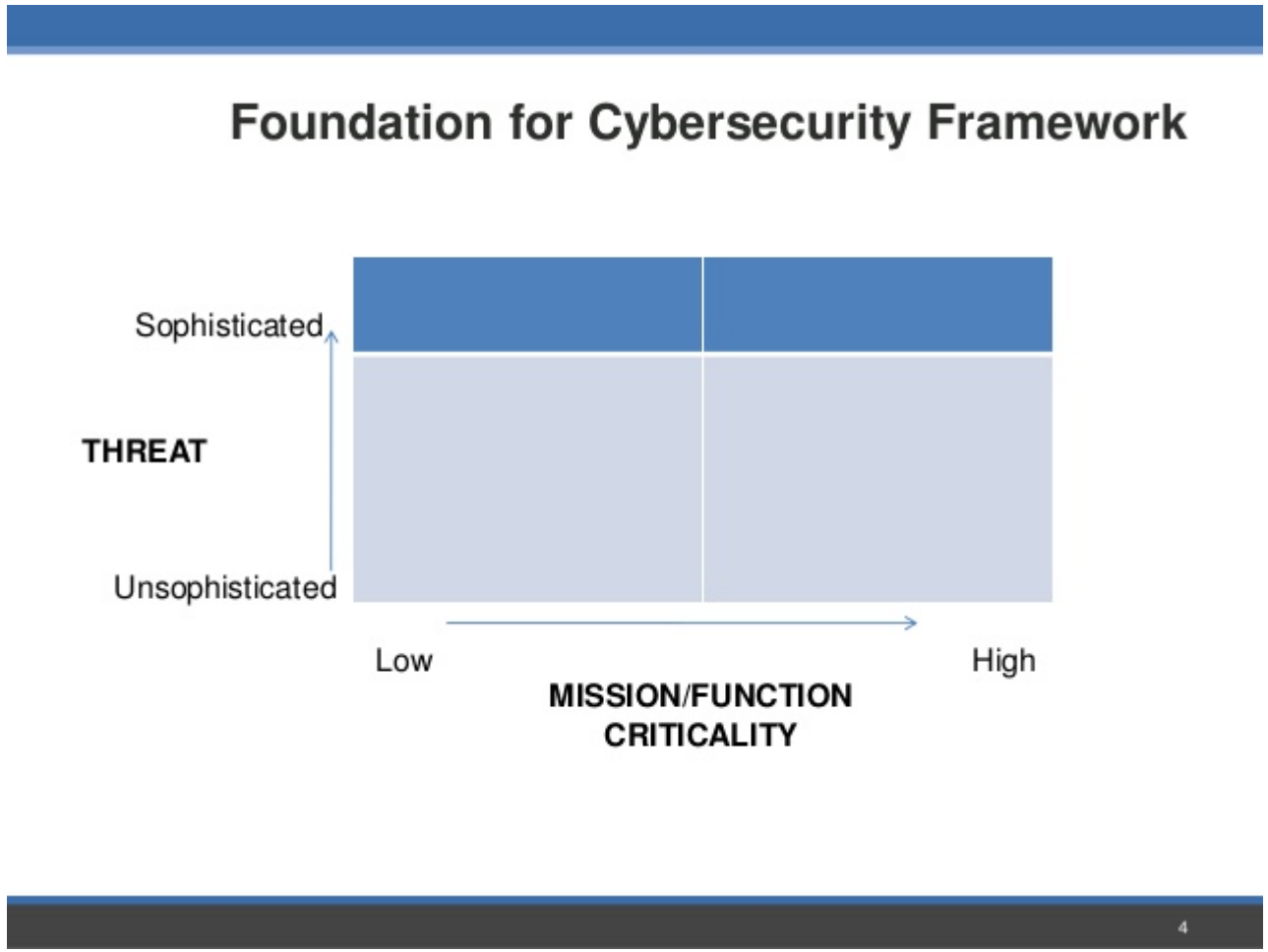
Cyber hygiene addresses ~80% of threats: Cyber hygiene refers to steps taken by users to maintain the health of their computers and devices and improve online security to prevent the theft or corruption of data. Further, as with personal hygiene, cyber hygiene should be practiced regularly to ward off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

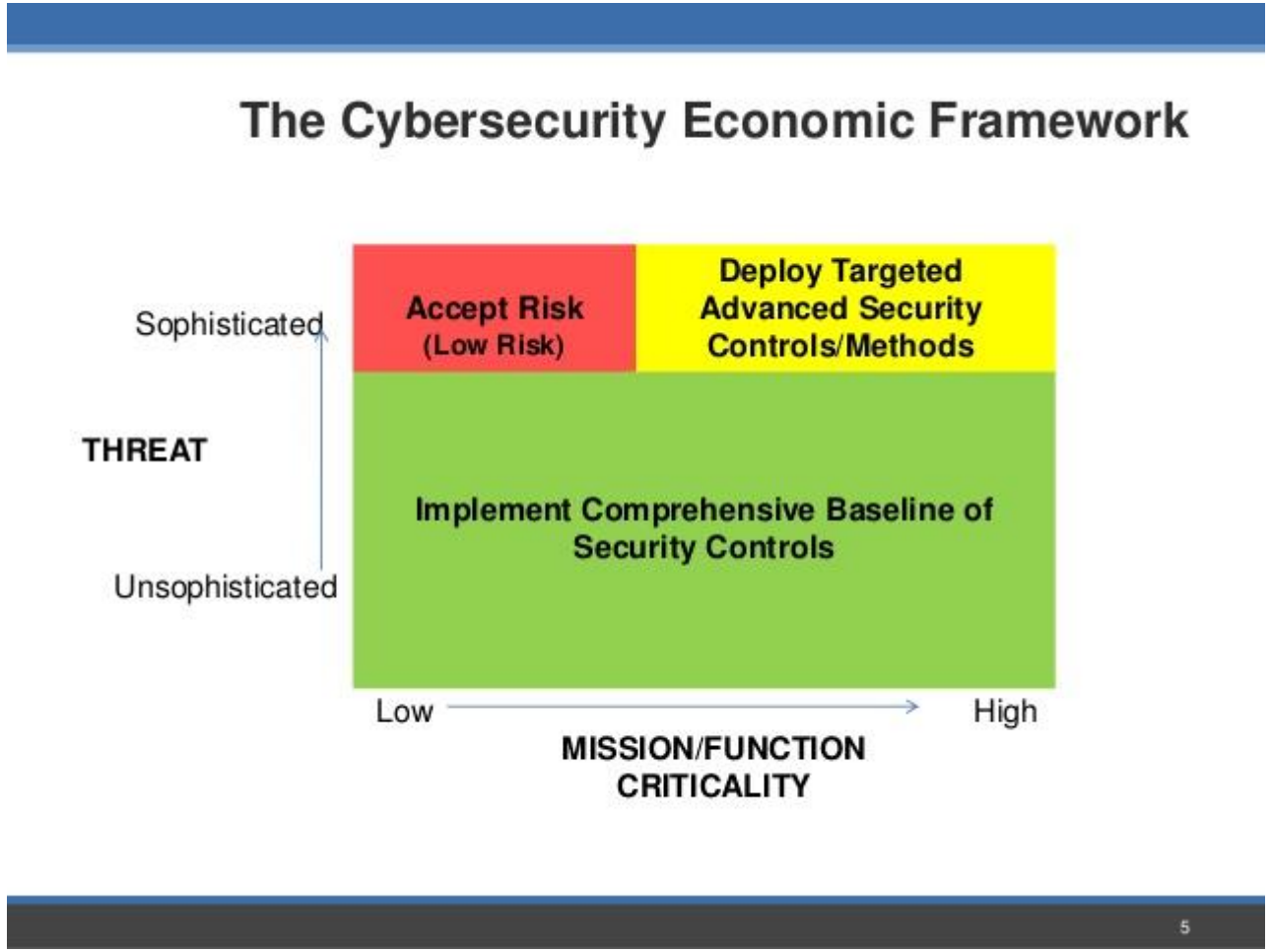
Addressing the 20% "gap" requires a fundamentally different approach:

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

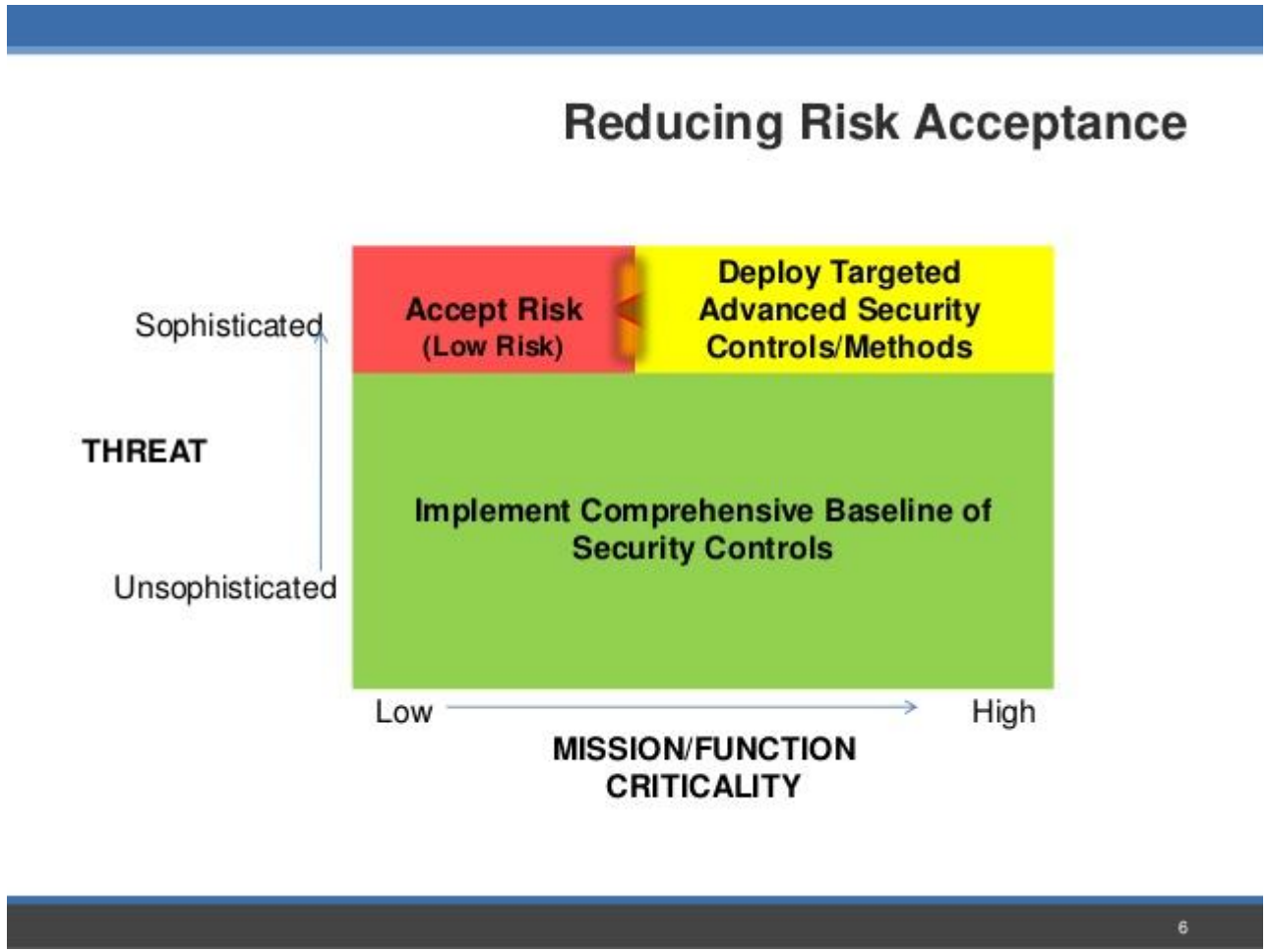
A foundation



A foundation (cont'd)



A foundation (cont'd)



A foundation (cont'd)

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

7

A foundation (cont'd)

Expanding Targeted Advanced Security Controls/Methods/Tools

Enhanced Descriptor	*Employment of Security Controls*	*Security Tailored 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

8

A foundation (cont'd)

Extended Cybersecurity Framework

Cybersecurity Framework Area	Employment of Security Controls	Security Tailored to Mission	Participate in Information Sharing (threat/vul)	Response to Cyber Threats
Deploy Targeted Advanced Security Controls/Methods	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
Implement Comprehensive Baseline of Security "Good Hygiene"	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

9

A foundation (cont'd)

Extended Cybersecurity Framework

Enhanced Descriptor	*Employment of Security Controls*	*Security Tailored to Mission*	*Participate in Information Sharing (threat and vulnerabilities)*	*Response to Cyber Threats*	*Cybersecurity Framework Area*
Level 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 Deploy Targeted Advanced Security Controls/Methods
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	
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 Security "Good Hygiene"
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	

10

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. **D**efine 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 •

A foundation (cont'd)

Metrics for Enhanced Cybersecurity

Enhanced Cybersecurity Framework Descriptor	*Employment of Security Controls*	*Security Tailored to Mission*	*Participate in Information Sharing (threat and vulnerabilities)*	*Response to 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 sophisticated 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 critical 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/Vulnerability information pushed to organization but inconsistently reviewed or applied	Metric: Attack response prompted from outside the organization

15

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 → 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

SMT
School of Management
and Technology
Business School des SCMT

SCMT
Steinbeis Center of Management
and Technology
Research | Education | Consulting

Steinbeis University
Berlin SHB