Cyber Space

Definition: At its essence, cyberspace is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online.

- Cyberspace is first and foremost an information environment. It is made up of digitized data that is created, stored, and, most importantly, shared.
- Cyberspace isn't purely virtual. It comprises the computers that store data plus the systems and infrastructure that allow it to flow.
- Cyberspace has also come to encompass the people behind those computers and how their connectivity has altered their society.
- One of the key features, of cyberspace is that its systems and technologies are man-made.
- It relies on physical infrastructure and human users who are tied to geography, and thus is also subject to our human notions like sovereignty, nationality, and property.
- Cyberspace, like life, is constantly evolving. The geography of cyberspace is much more mutable than other environments.
- The hardware and software that make up cyberspace, for instance, were originally designed for computers operating from fixed wires and telephone lines.
- Along with the technology of cyberspace, our expectations of it are likewise evolving.

  Thus, while cyberspace was once just a realm of communication and then e-commerce, it has expanded to include what we call "critical infrastructure." These are the underlying sectors that run our modern-day civilization, ranging from agriculture and food

distribution to banking, healthcare, transportation, water, and power. Each of these once stood apart but are now all bound together and linked into cyberspace via information technology.

Internet

The first thing your computer needs to know is how to find the servers that host the searched web page.

- To do that, it will use the Internet Protocol (IP) number that serves as the address for endpoints on the Internet. Your machine was most likely automatically assigned an IP address by your Internet service provider.
- Finally, your computer knows the address of a Domain Name System server.
  The Domain Name System, or DNS, is the protocol and infrastructure through which computers connect domain names to their corresponding IP address.

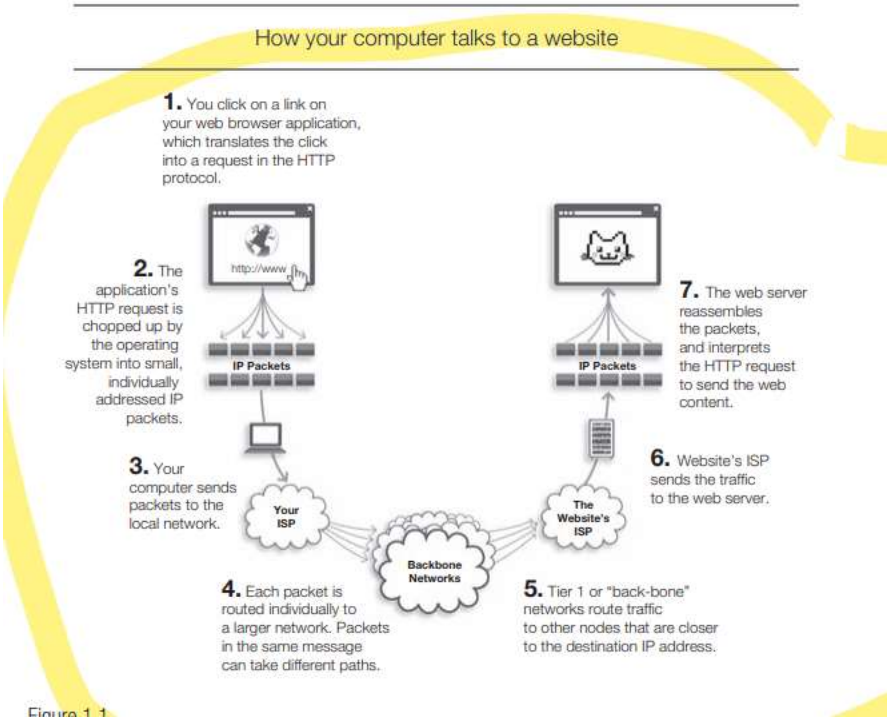

Figure 1.1

Figure 1.1 illustrates how your computer requests a web page by breaking down the request into packets and sending them across the Internet.

First, at the “layer” of the application, your browser interprets the click of your mouse as a command in the HyperText Transfer Protocol (HTTP), which defines how to ask for and deliver content. This command is then passed down to the transport and network layers.

Transport is responsible for breaking the data down into packet-sized chunks and making sure that all of the chunks arrive free of error and reassembled in the correct order for the application layer above.

The network layer is responsible for trying its best to navigate the packets across the Internet.

If you think of the data you are trying to send and receive as a package of information, the transport layer is responsible for packing and receiving the packages, while the network is responsible for moving them from source to destination. Once at the destination, the packets are reassembled, checked, and then passed back up to the application—in this case, a web server sending you the web content you requested.

The takeaway for cybersecurity is that the entire system is based on trust. It is a system that works efficiently, but it can be broken, either by accident or by maliciously feeding the system bad data.

Security and threats

When the difference between the expected behavior and actual behavior is caused by an adversary (as opposed to simple error or accident), then the malfunction is a “security” problem.

cyber problem only becomes a cybersecurity issue if an adversary seeks to gain something from the activity, whether to obtain private information, undermine the system, or prevent its legitimate use.

Traditionally, there are three goals: Confidentiality, Integrity, Availability, sometimes called the “CIA triad.

Confidentiality refers to keeping data private. Privacy is not just some social or political goal. In a digital world, information has value. Protecting that information is thus of paramount importance. Not only must internal secrets and sensitive personal data be safeguarded, but transactional data can reveal important details about the relationships of fi rms or individuals. Confi dentiality is supported by technical tools such as encryption and access control as well as legal protections.

Integrity is the most subtle but maybe the most important part of the classic information security triumvirate. Integrity means that the system and the data in it have not been improperly altered or changed without authorization. There must be confi dence that the system will be both available and behave as expected.

Availability means being able to use the system as anticipated. Here again, it’s not merely the system going down that makes availability a security concern; software errors and “blue screens of death” happen to our computers all the time. It becomes a security issue when and if someone tries to exploit the lack of availability in some way

Additional

Resilience. Resilience is what allows a system to endure security threats instead of critically failing. A key to resilience is accepting the inevitability of threats and even limited failures in your defenses.

Threats

Finally, it is useful to acknowledge when the danger comes from one of your own.

The "insider threat" is particularly tough because the actor can search for vulnerabilities from within systems designed only to be used by trusted actors.

Insiders can have much better perspectives on what is valuable and how best to leverage that value, whether they are trying to steal secrets or sabotage an operation.

It is also important to consider whether the threat actor wants to attack you , or just wants to attack.

Targeted Attack

Some attacks target specific actors for particular reasons, while other adversaries go after a certain objective regardless of who may control it.

Untargeted malicious code could, for example, infect a machine via e-mail, search for stored credit card details of anyone, and relay those details back to its master without any human involvement.

The key difference in these automated attacks is one of cost, both from the attacker's and the defender's perspective. For the attacker, automation hugely reduces cost, as they don't have to invest in all the tasks needed, from selecting the victim to identifying the asset to coordinating the attack.

Their attack costs roughly the same no matter how many victims they get.

A targeted attack, on the other hand, can quickly scale up in costs as the number of victims rises. These same dynamics shape the expected returns. To be willing to invest in targeted attacks, an

attacker must have a higher expected return value with each victim.
By contrast, automated attacks can have much lower profit margins.

The good news is that there are only three things you can do to a computer: steal its data, misuse credentials, and hijack resources. Unfortunately, our dependence on information systems means that a skilled actor could wreak a lot of damage by doing any one of those. Stolen data can reveal the strategic plans of a country or undermine the competitiveness of an entire industry.
Stolen credentials can give the ability to change or destroy code and data, changing payrolls or opening up dams, as well as the ability to cover tracks.
Hijacking resources can prevent a company from reaching customers or deny an army the ability to communicate.