Toward a Better Understanding of "Cybersecurity"

JEROEN VAN DER HAM, National Cyber Security Centre, The Netherlands and University of Twente

The term "cybersecurity" has gained widespread popularity but has not been defined properly. The term is used by many different people to mean different things in different contexts. A better understanding of "cybersecurity" will allow us a better understanding of what it means to be "cybersecure." This in turn will allow us to take more appropriate measures to ensure actual cybersecurity.

CCS Concepts: • **Security and privacy** → **Systems security**; **Human and societal aspects of security and privacy**; • **Social and professional topics** → *Management of computing and information systems*; History of computing;

Additional Key Words and Phrases: CIA triad, cybersecurity, vulnerability

ACM Reference format:
Jeroen van der Ham. 2021. Toward a Better Understanding of "Cybersecurity". *Digit. Threat.: Res. Pract.* 2, 3, Article 18 (June 2021), 3 pages.
https://doi.org/10.1145/3442445

1 INTRODUCTION

For many years a popular definition of cybersecurity has been the *CIA triad*: Confidentiality, Integrity, and Availability. In this column I argue that this definition can lead to a narrow view of cybersecurity. Instead, we should focus more on the activity and associated risks for cybersecurity. It is now time to let go of this ancient definition and seek better ways to define cybersecurity.

2 THE CIA TRIAD

The CIA triad, Confidentiality, Integrity and Availability, has been used as the practical definition of information security, and later cybersecurity, since the beginning of the field of cybersecurity. The tenet of the CIA triad is that cybersecurity of assets is defined by three different aspects:

(1) Confidentiality: information is only available to the intended consumers,
(2) Integrity: it is possible to prove that the information has not been changed,
(3) Availability: information should be available to the intended consumers.

The triad itself was introduced in the Anderson Report [1], which discussed security exposure, and repeated in Saltzer and Schroeder [5]. The CIA abbreviation was coined later by Steve Lipner around 1986 [2]. Since then, the term has been used widely in reports, standards, and other publications on cybersecurity.

Author's address: J. van der Ham, National Cyber Security Centre, The Netherlands, University of Twente, PO Box 117, 2501 CC The Hague, The Netherlands; email: j.vanderham@utwente.nl.

2576-5337/2021/06-ART18
https://doi.org/10.1145/3442445

2.1 Focus on the CIA Triad Aspects

The focus on the aspects defined in the CIA triad is problematic for several different reasons. The aspects are binary measures; at a given time they are either true or false. This sense of measurement gives a false sense of accomplishment, as the current status gives no guarantees about the future (or even the past).

The binary nature of these aspects is counterintuitive to risk assessment. Each aspect is taken as an absolute value that must be upheld, instead of performing a risk assessment that may impact the security of an asset.

The triad leads to a narrow focus on the security of individual assets. Confidentiality is a property of an individual asset, and usually not a property of a context, such as a computer network or office environment. This then leads to individual measures on objects instead of a general approach to cybersecurity.

The individual, binary measures and narrow focus in turn often lead to stop-gap solutions. Once a vulnerability threatens to break confidentiality, a measure is put in place to ensure confidentiality again. The actual risk associated with that vulnerability is then usually not taken into account. Due to the mitigation, confidentiality is now guaranteed again, so the problem appears to be solved. This is then often repeated many times for every new vulnerability.

Over the years, the CIA triad has been extended but has always retained a focus on aspects of assets. One of the first extensions has been to add “non-repudiation.” A later extension is the Parkerian hexad [4], with two other additional aspects, “possession” and “utility.” The fundamental problem of the focus on (binary) aspects of individual objects remains, however.

2.2 The Context has Evolved, the Approach to Security Has Only Minimally Adapted

In the advent of the cybersecurity field, risks associated with cybersecurity were poorly understood. When the CIA triad was proposed, computers were not connected to a (local) network, and the Internet did not even exist. Ware [6], Anderson, and Saltzer and Schroeder have done great theoretical work regarding computer security, since there were little to no practical attacks on computers.

The context in which we use computers has evolved significantly. From single, offline, room-filling computers, we now have multiple computers in our pockets that are constantly connected. Most processes in the physical world are now affected in some way or another by computers. The nature of adversaries have changed significantly.

Traditional security in the 1990s and early 2000s has been to provide security at the edges of networks. With the advent of mobile devices and the gaining popularity of bring your own device (BYOD) policies this approach was no longer tenable. The boundaries of security have moved with it, yet the overall approach to security has not. This has only strengthened the tendency to go for individualistic approaches to security.

3 NEW APPROACH TO CYBERSECURITY

With over 40 years of practice, we now have a better understanding of the risks for cybersecurity. We have been able to learn from many different kinds of incidents and attacks. So the risk models that we can create now are grounded in both theory and practice.

Yet, many practical and academic reports today still use the CIA triad as the definition of cybersecurity, while many newer approaches exist. As an example, consider the NIST cybersecurity framework [3].

3.1 The NIST Cybersecurity Framework

The NIST cybersecurity framework is defined as a set of five different activities. These activities are continuous, and the level to which these are performed depend on the organisation and its context. They are as follows:

(1) Identify: identify the assets that must be secured and the context that they are in
(2) Protect: define and implement protective measures for the assets
(3) Detect: put sensors and processes in place to detect when protection has been breached

(4) Respond: define response processes for when an incident has been detected
(5) Recover: develop plans for resilience in the organisation, as well as recovery mechanisms

With the identify activity all assets of an organisation that must be secured are identified. Creating this overview of all assets facilitates taking a more generic approach to security when assets are to be protected. Another important part of the identify activity is to examine the context of the assets, to consider what the assets must be protected, but also how the protective measures may impact existing processes.

Protect in the framework is only one of the activities instead of the main focus. This process puts the protective measures more into perspective and makes them part of an overall solution.

The Detect, Respond, and Recover activities force one to consider that security is never absolute. Some risks are just too costly to protect against and instead should be addressed by detection, incident response, and recovery activities. It also forces one to consider that security is never perfect, so other measures should be put in place to mitigate negative consequences of other protective measures that may fail.

3.2 More Appropriate Cybersecurity

Addressing cybersecurity as a an overarching activity instead of a binary measure creates more appropriate responses on cybersecurity. Appropriate in the sense that the defence fits the context and the actual risks identified instead of aiming for an absolute defence for each individual asset. Approaching cybersecurity as a general activity creates a better overview and facilitates a more concerted effort with different protectional measures.

Finally, viewing cybersecurity as a continuous activity allows organisations to better move with developments. Having identified each of the assets and having already done risk-assessments makes it easier to re-evaluate these in light of upcoming changes.

4 CONCLUSION

The CIA model has served as an important foundation for cybersecurity since the early 1980s. The triad served as a model for protecting digital assets when they were clearly distinguishable and separate entities. The CIA aspects are an important ingredient, but they should no longer be seen as the goal of cybersecurity.

The digital infrastructure has evolved significantly and now permeates almost all aspects of society. This means that cybersecurity cannot be an absolute goal but should be seen as a continuous activity that fits within a certain context. This in turn will allow for more natural risk assessments and a more general approach to cybersecurity. Once we take up this new definition, many more research questions will come up. Seeing cybersecurity as an ongoing activity also provides a better embedding of continuous risk assessment, while the world around us keeps changing and throwing up new threats. This view allows for a more realistic evaluation of measures instead of being limited to the CIA aspects.

REFERENCES

[1] J. Anderson. 1972. *Computer Security Planning Study.* Technical Report ESD-TR-73-51. Air Force Electronic System Division.

[2] Steve Lipner and Ross Anderson. 2018. CIA history. *Personal communication.*

[3] NIST 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* Technical Report. National Institute of Standards and Technology. DOI: https://doi.org/10.6028/nist.cswp.04162018

[4] Donn B. Parker. 1983. *Fighting Computer Crime.* Scribner, New York, NY.

[5] J. H. Saltzer and M. D. Schroeder. 1975. The protection of information in computer systems. *Proc. IEEE* 63, 9 (1975), 1278–1308. DOI: https://doi.org/10.1109/proc.1975.9939

[6] Willis H. Ware. 1970. *Security Controls for Computer Systems.* Technical Report. RAND Corp. Snta Monica, CA.

Received March 2020; revised November 2020; accepted December 2020