**EMCS2200:** Global Cyber Challenges: Law, Policy, and Governance

Assignment: Cybersecurity Policy Agenda Paper

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

Drafted : 1/12/2019

Finalized: 2/9/2019

#### Proposal for a **Live Technology Definition Database** ( LTDD )

#### Introduction

Mr. President, as a response to reports that our nation is ill prepared to defend itself against CyberAttacks, many groups have proposed all types of policies and strategies. These policies, if enacted, would require broad among agreement among allies and adversaries if enacted internationally, or require hard coordinate cooperation between business and government if enacted domestically. Furthermore tricky cross functional oversight during implementation and the need for careful ( and sometimes intrusive ) ongoing monitoring makes even the most innovative policies susceptible to catastrophic failure. However, our committee has found a more fundamental weakness that would affect all policy making efforts : Technology Definitions. It may seem trivial but a technical definition, especially one that is legally binding, can make a difference between a strong cybersecurity policy and one without very little power to enact the change it seeks to propagate. Furthermore strong ubiquitous definitions when shared across and throughout the government help to build a network of common understanding, the type of understanding needed to help policies work in concert with each other, instead of causing conflicts and confusion. Creating a firm resolve to solve complex cybersecurity problems requires an equally firm resolve to create consensus around the definitions of the assets and protocols we are protecting.

#### The Problem

It might not be obvious to the uninitiated but the world of software engineering is immense and complex. Even though software, as we know it, has only been around for maybe 70 years, it has evolved more rapidly than anyone could have predicted. Software is growing fast and becoming exponentially complex at a high velocity. Therefore, it's no surprise that law, policy, and regulation struggle to keep up, especially in a legal system where “stare decisis” is coveted above any type of agreed upon morality, common sense or logic. The fact is that we depend on legal precedent to interpret the meaning of the lofty ( and often vague ) language found in The US Constitution, reveals a fatal flaw. In the non-technical world it feels O.K. for us to wait till “something happens” that challenges current rules, laws, norms or regulation, before we allow it make its way through the layers of our judicial system and finally deal with it. However, with technology the damage that can be done in the space of a year or 6 months could create its own precedent and convention, one that may be counterintuitive to our moral fabric or safety. And while it may be impossible preemptively make laws or regulation for technology that doesn’t exist, we can do better in the way of actively creating legal classifications for the technology that does exist. In fact, the lack of standardization among technology definitions across agencies, courts and departments causes a great amount confusion, inconsistent ( and possibly unequal ) enforcement and less than adequate implementation of cybersecurity regulation, policy and law. Legal precedent will never move faster ( or fast enough ) to keep up with the evolution of technology unless we create a legal framework that recognizes a shared body of information as legal technology definitions based on open professional standards. Therefore, we propose the creation of such a body of information, one that we will refer to as the **Live Technology Definition Database** or LTDD. While this body of information does not tell us whether something is a crime or not, it at least helps us carefully define what things are in the world of technology so we can have unified and cohesive language when trying to describe the ecosystem in which people, companies, and law enforcement operate.

#### The Solution

Since almost all of the technology definitions we need already exists in Wikipedia ( or in some other place ) where it can be easily referenced, why make it into law? This is true, Wikipedia is full of very complete and credible technical definitions. However, it is unclear where agencies, courts or branches of the military for example, find or formulate their definitions in regards to technology and more importantly cybersecurity. Furthermore it's also unclear if they share definitions with each other or require proper vetting of the definitions before including them in internal policies. During legal proceeding in our courts “experts” are often brought in to testify about things that might be confusing for a jury. Who is to say that one expert’s opinion accurately speaks for the industry, or even for a small section of the industry like a specific coding language? How, for example, would a non-technical jury being overseen by a non-technical judge make a judgement on whether a key technical component in a CyberSecurity case was credible or not. Is this simply left to whichever lawyer is most persuasive? In situations where the prosecution and the defense each bring in their own expert, how is a non-technical jury member supposed know if one of the “experts” is completely fraudulent if there is no baseline technical classification? Since there is no legal definition for code or code systems, often the expert who is more persuasive is the person people believe. This is problematic because we all know that persuasion doesn’t equal truth.

By making the LTDD into law, and formulating a policy that requires agencies and courts to reference the information in the LTDD when creating their strategy or formulating legal decisions we accomplish some very important things:

1. Government Agencies and the Military will have one shared vernacular, one created by professionals and blessed by the United States Government, which will be an essential tool during the creation internal policy.
2. It forces agencies to address the threat related definitions when considering their internal and external policies in a way that tracks with current commercial knowledge and usage, eliminating the sense that the law are always “behind the curve.”
3. It helps make the work of the Judicial Branch more accurate by providing a comprehensive, cross referenced, vetted body of work ( much like a legal dictionary ), that provides a starting place for forming arguments and legal opinions.

#### Participants

The LTDD should be a diverse body of professionals of mostly technical experts from all areas of technology. Government, Commercial and Military representation should be equal and a leadership board should maintained in a way that does not give any one sector of the organization power over the others. When drafts of definition are made they should follow a consensus model ( modelled after Wikipedia and described below ).

#### Usage of the LTDD

When implemented, the LTDD should be considered law, meaning it is the accepted technical legal standard by which the law should be interpreted, in the way that we accept the dictionary is a valid representation of what words mean. This introduces a problem with previous decisions if the definition of technology differs from already settled case law, it could trigger a landslide of appeals. But, this is already the case with new decisions that create new precedents. Furthermore, if we are scared of overturning decisions that may have been bad because of the definitions of technology were bad, then we are accepting a static and non-progressive legal system, one that will not protect us from crimes or judicial overreach in a quickly evolving technology landscape.

Actual usage might look like this. Instead of just describing a circumstance as “a breach followed by the exfiltration of data”, the referencing the LTDD the circumstance will be described as “level 3 external breach followed by the exfiltration of level 3, type 6 data”, where the level references the sensitivity of the assets and type describes the categories of the assets. ( Of course the definitions don't have to include numbers, it could be categorized used named descriptors ). In this example, by referencing the LTDD the definitions of data and breach can be more precise, so we can differentiate between “data” used to decide the color theme of a website and the credit card data.

#### Practical Considerations

**Who Will Operate and Manage The LTDD** : As a matter of governance the LTDD should be run by a diverse group of people with varying levels of experience but all recognized as leaders in their respective fields under the umbrella of MITRE. Currently MITRE is organized with the following scope of responsibility:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Center** | **Sponsored by** | **Scope** | **Established** | **Refs** |
| [National Security Engineering Center](https://en.wikipedia.org/w/index.php?title=National_Security_Engineering_Center&action=edit&redlink=1) | [Department of Defense](https://en.wikipedia.org/wiki/United_States_Department_of_Defense) | National security issues |  | [[4]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-4) |
| [Center for Advanced Aviation System Development](https://en.wikipedia.org/w/index.php?title=Center_for_Advanced_Aviation_System_Development&action=edit&redlink=1) | [Federal Aviation Administration](https://en.wikipedia.org/wiki/Federal_Aviation_Administration) | Air traffic management | October 1, 1990 | [[5]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-5)[[6]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-6) |
| [Center for Enterprise Modernization](https://en.wikipedia.org/w/index.php?title=Center_for_Enterprise_Modernization&action=edit&redlink=1) | [Internal Revenue Service](https://en.wikipedia.org/wiki/Internal_Revenue_Service) and [Department of Veterans Affairs](https://en.wikipedia.org/wiki/United_States_Department_of_Veterans_Affairs). | Enterprise modernization | July 1998 | [[7]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-7)[[8]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-50years-8) |
| [Homeland Security Systems Engineering and Development Institute](https://en.wikipedia.org/w/index.php?title=Homeland_Security_Systems_Engineering_and_Development_Institute&action=edit&redlink=1) | [Department of Homeland Security](https://en.wikipedia.org/wiki/Department_of_Homeland_Security) | To safeguard people in the United States against terrorist threats, aid the flow of legal commerce and immigration, and recover swiftly from natural disasters and other national emergencies | March 6, 2009 | [[9]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-9)[[10]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-10) |
| [Judiciary Engineering and Modernization Center](https://en.wikipedia.org/w/index.php?title=Judiciary_Engineering_and_Modernization_Center&action=edit&redlink=1) | [Administrative Office of the United States Courts](https://en.wikipedia.org/wiki/Administrative_Office_of_the_United_States_Courts) |  | December 2, 2010 | [[11]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-11)[[12]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-12) |
| [CMS Alliance to Modernize Healthcare](https://en.wikipedia.org/w/index.php?title=CMS_Alliance_to_Modernize_Healthcare&action=edit&redlink=1) | [Centers for Medicare and Medicaid Services](https://en.wikipedia.org/wiki/Centers_for_Medicare_and_Medicaid_Services) |  | October 2012 | [[13]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-13)[[14]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-14) |
| [National Cybersecurity FFRDC](https://en.wikipedia.org/wiki/National_Cybersecurity_FFRDC) | [National Institute of Standards and Technology](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) |  | September 24, 2014 | [[15]](https://en.wikipedia.org/wiki/Mitre_Corporation#cite_note-15) |

We propose that the LTDD fall under the management of the Judiciary Engineering and Modernization Center with a dotted line to the National Cybersecurity FFRDC.

**How Will The Information in The LTDD be Formatted** : The formatting of the information should mimic Wikipedia is style and content. There should be heavily cited entries that constitute the facts, followed by examples and along with a section that discussing controversial ideas or ideas that are unsettled.

**How Will Consensus Work in The LTDD** : We recommend the Wikipedia method for creating consensus. “Decisions on Wikipedia are primarily made by consensus, which is accepted as the best method to achieve Wikipedia's goals, i.e., the five pillars. Consensus on Wikipedia does not mean unanimity (which is ideal but not always achievable), neither is it the result of a vote. Decision making and reaching consensus involve an effort to incorporate all editors' legitimate concerns, while respecting Wikipedia's policies and guidelines.” [[1]](#footnote-0)

#### Technology Axioms

Technology axioms are definitions that are accepted as foundation truths, truths that do not require further definition. This is not to say that an axiom cannot be challenged, however, challenging an axiom should not be a simple task. Examples include:

Definitions of what programming is, or what code is.

Definitions of what a computer network is, or what constitutes a cloud service.

Definitions of when code is considered to be malware.

It will be very hard to NOT cross the line into policy, like creating a definition that describes when a user should be informed when a site privacy policy changes. Instead we will encourage the writer to define what a website is, and the various technical ways that site privacy policies may be delivered. The purpose of the LTDD is make sure we have a clear consensus of the WHAT with the intent of making clarity on the SHOULD easier to figure out when legal situations arise.

#### Core Definitions

A core definition is a definition that describes established technology. These definitions would include:

Definitions that **delineate programming languages**[[2]](#footnote-1). We mentioned in the overview that there are over 300 recognized programming languages, but looking at a *generational* list there are really only about 26, with branches of versions and divisions among them. And since the main objective of the LTDD is classification for legal purposes, we can safely say that handling the classification definitions for 26 languages is very practical and highly obtainable.

Definitions that describe **how security in different programming languages and platforms work** ( they are all different ) along with a current list of known vulnerabilities in each version.

Core definitions are important. Who is to say that you shouldn’t write code to protect your website using CSS? Well several reasons to make the case against using CSS to provide security could be made by using information in the LTDD. By definition of what they are, certain technologies are not well suited for use as security measures. And this is not a matter of opinion, this can be delineated with facts.

#### Process Definitions

Process Definitions describe how things are done in the world of technology, especially processes that constitute protocols such as HTTP or TLS. Examples of process definitions include :

Descriptions of how packets are transferred from one machine to another.

Descriptions of how communication may be encrypted and decrypted.

Descriptions of how a compiler converts a developer code into code that can be used by a machine.

Descriptions of how memory management works in compiler frameworks.

By defining the processes and protocols we are provide a baseline of understanding for discussions about the security for these processes and protocols. When the topics are complex, it helps to have a authoritative source to reference, rather than competing “theories” on the same subject.

#### Data Asset Definitions

Data asset definitions will probably be most important work of the LTDD. All data is not created equal, especially when it is or can be linked to personally identifiable information. Right now some may argue there is a loophole in the law as it relates to meta-data, which according to current US law is not confidential or protected by the 4th Amendment.[[3]](#footnote-2) However is unclear if this designation is still technically sound or legally enforceable.[[4]](#footnote-3) This confusion will not be solved by legal precedent unless the judicial branch intends to try cases for all of the ways data can be classified, stored or collected in the next 12 months. Once again, there are too many variants of the same thing that change too quickly to wait for legal precedent. While the LTDD will not settle the issue of the ways policy and laws are applied, the LTDD will clarify what data is or is not. Here are some key definitions:

Classifications of data sensitivity as it relates to privacy.

Classification of data storage methods.

Classification of data encryption methods.

These three classifications will give a baseline for understanding data exponentially better, so we can apply the law in a more precise manner.

#### Attack and Breach Classifications

Attack and breach classifications like data definitions will most likely be the most referenced definitions of the LTDD because they define the anatomy of an attack or breach. In this section researchers will use forensics from decades of attack data to model well known penetration methods and their variants. For example, “Password Stuffing” is a well known strategy, where attackers steal a password then try to break into multiple accounts with the same credentials in hopes that people reuse the credentials. By memorializing the description of the attack in a way that satisfies legal and technical requirements, the government can uniformly require agencies, departments and branches to implement practices that defend against this attack without the worry of each agency defending against their interpretation of what the attack was or an outdated model of the attack.

#### Personnel Definitions

Personnel Definitions will most likely be the most fluid of of all the definition categories, nonetheless it is an important one. While there is no legal obligation to follow the definitions in the LTDD, the definition provides other non-technical bodies and organizations a basic understanding of how work in technology community is divided among personnel, who generally bears the responsibility for different parts of the application stack, and type of expertise and knowledge ( for liability purposes ) that is generally required to perform a certain job. This is the first step to creating a requirement for federally certified software engineers, much in the way that we require Doctors, Lawyers, Insurance Agents, Stock Brokers and Pilots to obtain some type of certification.

#### Threat and Vulnerability Definitions

There are informal organizations that track vulnerabilities and threats, but only one with formal recognition from the US Government. “The National Cybersecurity FFRDC (NCF) is a federally funded research and development center operated by MITRE Corporation. It supports the U.S. National Institute of Standards and Technology's National Cybersecurity Center of Excellence. NCF is the first and, as of March 2017, only federally funded research and development center dedicated solely to cybersecurity.”[[5]](#footnote-4)

The MITRE Corporation doesn’t create law, but it serves as a good first step toward creating, collating and processing the type of information we need across the country in the effort to create a cohesive body of cyberware intelligence. If the LTDD was a division of the MITRE corporation or administered by the MITRE corporation it would provide adequate oversight for the project.

#### Conclusion

Maintaining a database of baseline technology definitions may not seem as powerful as a body of laws regulating CyberSecurity, but a body of laws regulating CyberSecurity without a cohesive body of definitions is equally useless. Much of the policy that current exists tries to define the law AND also define the terms in the same document and does not seek build from previous policies that may also include their own definitions . And, each time a new policy is formed it defines these terms again without reference previous documents. This lack of cohesion makes consensus almost impossible.

Creating the LTDD will be a significant amount of work, maintaining it will also be challenging. But if done right, it would be the first authoritative source for comprehensive knowledge on an an industry that touches almost every aspect of American life.

Works Cited

"Consensus." Wikipedia. January 09, 2019. https://en.wikipedia.org/wiki/Wikipedia:Consensus.

"Generational List of Programming Languages." Wikipedia. December 22, 2018. https://en.wikipedia.org/wiki/Generational\_list\_of\_programming\_languages.

"National Cybersecurity FFRDC." Wikipedia. May 10, 2018. https://en.wikipedia.org/wiki/National\_Cybersecurity\_FFRDC.

"O'GRADY v. Superior Court, 139 Cal. App. 4th 1423, 44 Cal. Rptr. 3d 72 – CourtListener.com." CourtListener. Accessed February 09, 2019. https://www.courtlistener.com/opinion/2305468/ogrady-v-superior-court/.

"Stored Communications Act." Wikipedia. February 01, 2019. Accessed February 09, 2019. https://en.wikipedia.org/wiki/Stored\_Communications\_Act.

1. “Consensus.” *Wikipedia*, Wikimedia Foundation, 9 Jan. 2019, en.wikipedia.org/wiki/Wikipedia:Consensus. [↑](#footnote-ref-0)
2. “Generational List of Programming Languages.” *Wikipedia*, Wikimedia Foundation, 22 Dec. 2018, en.wikipedia.org/wiki/Generational\_list\_of\_programming\_languages. [↑](#footnote-ref-1)
3. "Stored Communications Act." Wikipedia. February 01, 2019. Accessed February 09, 2019. https://en.wikipedia.org/wiki/Stored\_Communications\_Act. [↑](#footnote-ref-2)
4. "O'GRADY v. Superior Court, 139 Cal. App. 4th 1423, 44 Cal. Rptr. 3d 72 – CourtListener.com." CourtListener. Accessed February 09, 2019. https://www.courtlistener.com/opinion/2305468/ogrady-v-superior-court/. [↑](#footnote-ref-3)
5. “National Cybersecurity FFRDC.” *Wikipedia*, Wikimedia Foundation, 10 May 2018, en.wikipedia.org/wiki/National\_Cybersecurity\_FFRDC. [↑](#footnote-ref-4)