Does Cybersecurity Legislation Make us Safer Online?

An Analysis of the Impact of Consumer Related Cybersecurity Legislation on Device Security and Data Protection

Iain Nash[1]

16 August 2020

1 Introduction

'Cybersecurity is an often abused and much misused term that was once intended to describe and now serves better to confuse'

Herr and Friedman (2015)[2]

Marvin Minksy, one of the early pioneers of the study of Artificial Intelligence coined the phrase 'suitcase word' to describe phrases which by themselves mean little, and have to be unpacked in order to be understood.[3] Furthermore, the words within the 'suitcase' may create an association with a concept or an idea, despite the detail of the word being often quite intangible and non-attributable to a unique source. Minksy originally used the term to describe words such as intelligence or consciousness, and the term has gone on to be used to identify when people grapple with generalised topics via shorthand, but risk uniting a distinct set of concepts which don't actually overlap.[4] Cybersecurity has become such a suitcase word, and its use has become so commonplace that its meaning has become generalised and devoid of specific intent, although it does retain a generalised objective.

Despite the scope creep associated with the word, the canonical definition of cybersecurity is quite simple. In its original form, cybersecurity was defined as the measures used to ensure the *confidentiality*, *integrity* and *availability* of electronic information.[5] Provision of this 'CIA Triad' means that information remains private, correct and available for use and the actions taken in ensuring this outcome fall under the umbrella of 'cybersecurity'.

However, the term is now found regularly in, and has become closely associated with, disparate topics such as, *inter alia*, policy discussions, legislation, offensive and defensive military operations, data protection, privacy concerns and cybercrime operations. There remains still, both an academic and professional industry built upon the furtherance of technical methods to help ensure the CIA of electronic systems, but it is no longer the case that the term can automatically be taken to refer its original definition. Furthermore, given

[1] School of Law, Queen's University Belfast. inash01@qub.ac.uk. The author thanks the contributions and support from Prof. Daithi Mac Sithigh and Dr. Philip O'Kane, as well as comments from Dr. Bruce Schneier.

[2] Trey Herr and Allan Friedman, 'Redefining Cybersecurity' 2015 8 Defense Technology Program Brief (The American Foreign Policy Council)

[3] Marvin Minksy, *The Emotion Machine: Commonsense Thinking, Artificial Intelligence, and the Future of the Human Mind* (Simon & Schuster, Inc. 2007)

[4] Zachary C. Lipton and Jacob Steinhardt, 'Troubling Trends in Machine Learning Scholarship' (Thirty-Fifth International Conference on Machine Learning)

[5] Peter W. Singer and Allan Friedman, *Cybersecurity & Cyberwar* (Oxford University Press 2014) 35

how we now interact with many Smart Devices,[6] and the fact that these devices can now have a physical impact on our property and person, cybersecurity no longer remains focused solely on the protection of information but can now be considered as a form of physical protection also.[7] Indeed, when it comes to Smart Devices, cybersecurity has become synonymous with product safety.

This author believes that given the esoteric nature of cybersecurity (in its original form) and because of its highly technical subject matter, debate on the topic of cybersecurity by non-technical discussants has become somewhat reduced to 'the protection of computers' at scales measuring from distinct individual devices to groups of networks. The nebulousness of this discussion has allowed the drafting of both policy and legislation which includes references to cybersecurity but which have little specific guidance with regard to the subject, and indeed it could said that the term is now implies 'the unspecified actions taken by other people to attempt to protect software, devices, networks or network systems'. As a result of the broad (over)reach and lack of precision associated with the term, this paper attempts to examine legislation which refers to, directly or indirectly, cybersecurity and determine if the legislation can be objectively said to make us safer online in a non-trivial way.

In order to perform this assessment, a framework has been developed, through which cybersecurity legislation is viewed and assessed. This framework comprises of four distinct elements which map to the intent and specific meaning implied by each distinct cybersecurity reference within legislation and allows for the differentiation between the practical aspects of cybersecurity and policy from the wider policy and non-practical connotations which have become associated with the term, while also assessing both the intent and the object of the underlying legislation. Furthermore, the framework was developed with the intent of allowing for a comparison and assessment between distinct pieces of legislation, which may use different terminologies and rely on differing core assumptions.

Within the paper, cybersecurity legislation from the European Union, the United States of America, Taiwan and a number of African countries is analysed.

2 What is online safety?

In order to answer the question posed by this paper, there must be a clear definition of 'safer'. From the definition of the term cybersecurity, we know that it is comprised of three primary elements; Confidentiality, Integrity and Availability. For the purpose of clarity within this discussion, two heuristics are used. Firstly, specific reference is made to an information system throughout the paper, but the principles discussed can apply to any operating system or network. Secondly, the subject of hypothetically proposed compromises is 'data'. Data in this context can mean, either in part or in full, the operating system(s), applications contained within the operating system, non-Personally Identifiable Information and Personally Identifiable Information. Finally, the 'us' in the question 'Does cybersecurity

[6] A Smart Device is a product which has both a CPU and an internet connection.

[7] See, for example, Mohmmed Nasser Al-Mhiqani and others, 'Cyber-security Incidents: A Review Cases in Cyber-Physical Systems' 2018 9 International Journal of Advanced Computer Science and Applications 499

legislation make us safer online' refers to consumer users of information systems, and therefore the impact on safety can be classified as either a 'first order' effect, which is where the consumer benefits directly from the legislation in the use of the devices or a 'second order' effect which can be summarised as a measure which improves the cybersecurity of an entity which the consumer relies upon, but over which the consumer cannot exercise control.

In order to assess the relative safety of an information system, it is necessary to break down the CIA triad into its individual components.

Safety arising from *confidentiality* comprises of two stages; the first is that the data which is stored is protected from being accessed by non-authorised actors, and the second is that, when the data which has been made accessible to a third party, this fact is presented to the operator the information system. This is particularly salient when the accessed data is Personally Identifiable Information and the subject of the data is informed when their data has been accessed so that they may take mitigating actions which are independent of the compromised system.

It is not possible to compromise the *integrity* of data within an information system without first compromising its confidentiality. In the parlance of system administration, compromising the integrity of an information system's data requires a higher level of 'privilege' than simply accessing it. Two fundamental privileges, which can be granted to users in any operating system are *Read* and *Write* access, and so a failure to preserve the integrity of a datum is the result of the granting of 'Write' access to an unauthorised party in addition to 'Read' access. This outcome is called a 'privilege escalation' and the granting of 'Write' access will enable the attacker to alter or delete existing data and to introduce new data to the system. Granting of 'Write' access can, in effect, give the attacker control over a system and its data. It is often the goal of a hacker to seek global write access within a system, as this will grant full control over the system. If this isn't possible, the hacker may just have limited Write access and is able to control a subset of the system.

Accordingly, we can see how failure to maintain the integrity of the system is more serious than failing to maintain its confidentiality, as the consequences can result in the system itself being subverted to the intent of the unauthorised party as opposed to just providing the unauthorised party with the information contained within the system.

Unlike Confidentiality or Integrity, a failure of *availability* does not necessarily require the third party to have compromised the confidentiality or integrity of the system. It is possible to deny a valid user access to a system by overloading or 'flooding' the system with access requests, which will prevent the system from processing genuine access requests and thus limiting or removing the ability of a user to access and avail of data in the system. This is commonly referred to as a 'Denial of Service' attack, and when this type of attack is carried out by a botnet, it is called a 'Distributed Denial of Service Attack'. It must also be noted that the effect of such attacks is usually temporary, as the only way to permanently deny access to data is to compromise its integrity and either delete or alter it.

Therefore, we can see how Confidentiality and Integrity are interlinked and hierarchical, while Availability is distinct, and in an objective assessment would rank below confidentiality or integrity because of its temporary nature. It should also be clear that, at a high and quite simplified level, the focus of cybersecurity actions related to the preservation of Confidentiality are aimed at preventing access to a system, while the focus of the preservation of Integrity is to limit the scope of the attacker to cause damage once access to the system has been gained. The focus on the preservation of Availability can be considered as access regulation and can be seen as one step removed from the data itself.

So far in this analyses, it would appear that the exercise of cybersecurity is a purely technical one, however, successful cybersecurity practices require both the technical programs and system architecture to follow security principles, as well as the users of the systems to follow good practices. Breitinger, Tully-Doyle and Hassenfeldt (2019), in an analysis of previous work on this subject note how among the general population there is a lack of awareness with regard to cybersecurity practices in relation to their mobile phones, but this finding does not hold for more tech savvy users.[8] Their survey finds that there hasn't been a material improvement in the use of cybersecurity principles by users over the past ten years, and that apart from the use of lock screens to secure physical access to their devices, the majority of users do not follow best practice when it comes to securing their devices. These results have been replicated in other empirical studies,[9] and work by Eichelberg, Kleber and Kammerer (2020) identify human error as a primary risk for the introduction of malware and malicious code into medical IT systems,[10] and Schneier (2018) notes how the director of the National Security Agency's offensive hacker team outlines how rather than rely on technical tools to gain access to systems, they often target an individual to obtain their credentials.[11]

Therefore, any legislation which is focused on increasing safety must have requirements which simultaneously both limit the scope of a user, either inadvertently or deliberately, to circumvent the aforementioned CIA requirements, as well as training for users on how to interact with information systems on a secure basis. Over-reliance on training or policy, combined with a failure to sufficiently compartmentalise and protect information allowed for whistleblowers such as Edward Snowden, Bradley Manning and the unidentified source behind the 'Panama Papers' leak to access, remove and publish information from the networks which they had access to.[12] This demonstrates how cybersecurity must be both a technical exercise, focused on both unauthorised third parties as well as authorised users, as well as a psychological exercise where users are trained and encourage to act in a secure manner.

---

[8] Frank Breitinger, Ryan Tully-Doyle and Courtney Hassenfeldt, 'A survey on smartphone user's security choices, awareness and education' 2019 88 Comput Secur 101647

[9] See, for example, Pintu Shah and Anuja Agarwal, 'Cybersecurity behaviour of smartphone users in India: an empirical analysis' 2020 ahead-of-print Information Comput Secur

[10] Marco Eichelberg, Klaus Kleber and Marc Kämmerer, 'Cybersecurity Challenges for PACS and Medical Imaging' 2020 Acad Radiol

[11] Bruce Schneier, *Click here to kill everybody* (W.W. Norton & Company 2018) 45

[12] See, for example, Edward Snowden, *Permanent Record* (1 edn, Macmillan 2019), Thomas Olesen, 'The Politics of Whistleblowing in Digitalized Societies' 2019 47 Polit Soc 277 and Michael R. Touchton and others, 'Whistleblowing or leaking? Public opinion toward Assange, Manning, and Snowden' 2020 7 Res Politics

3 Cybersecurity Contexts

It is common to find examples in the academic literature that view cybersecurity through the prism of both military operations and national security.[13] Accordingly, it would be remiss to not include the approach of Nation States to cybersecurity in any analysis of the subject.

Broadly speaking, the approach of Nation States to cybersecurity can be split into two categories – offence, which covers the actions of state-backed entities who are trying to compromise a system belonging to Nation State B because it is in the interest of Nation State A to do so; and defence, where actions are taken to prevent Nation Sate B from compromising Nation State A's own information systems. Although the offensive and defensive approaches are theoretically diametrically opposed, in practice they relate to the same underlying information systems and the cybersecurity approaches taken to defend them.

Egloff (2020) outlines three well known cyberattacks which have been attributed to Nation States (albeit denied by the states accused of perpetrating the actions); the 2014 hack of Sony Pictures, claimed to be the work of North Korea, the 2016 hack of the Democratic National Committee servers and the 2017 NotPetya attack, the latter two being attributed to Russia.[14] These attacks demonstrate how 'cyberwar' between Nation States no longer remains a theoretical exercise, although as Herr and Friedman (2015) note, military operations are conducted with the intent to inflict either permanent or long-term damage on their victim,[15] and it is not clear if military cyberoperations, perhaps with the exception of Stuxnet which was developed to slow down the impact of the Iranian nuclear program,[16] can be considered either as permanent or long-term. Even cyberattacks such as *WannaCry* and *NotPetya*, although resulting in billions of dollars' worth of damage were temporary in nature but still had a material impact upon Nation States. Brenner (2011) outlines a hypothetical example of permanent damage when he describes how a simulated cyberattack is able to cause a catastrophic failure of a power turbine resulting in an explosion,[17] but it is the belief of the author that by any objective standards, cyberweapons which can impact the day-to-day lives of people at a large scale should be included within the definition of cyberwar, even if direct effect of their actions is only temporary.

Accordingly, the point should now be clear that any engagement in cyberoffensive operations by a Nation State leads to a general requirement for increased cybersecurity. The reasons are twofold; firstly Nation States have the ability to hire and fund experts at developing both offensive and defensive capabilities and are able to deploy very large budgets to support these teams,[18] which will result in the development of techniques to

[13] See for example, Hsini Huang and Tien-Shen Li, 'A centralised cybersecurity strategy for Taiwan' 2018 3 J Cyber Policy 1, and Ruben Elamiryan and Radomir Bolgov, 'Comparing Cybersecurity in NATO and CSTO: Legal and Political Aspects' (GigaNet: Global Internet Academic Network, Annual Symposium 2018)

[14] Florian J. Egloff, 'Contested public attributions of cyber incidents and the role of academia' 2020 41 Contemp Secur Policy 55

[15] Herr and Friedman (n 2)

[16] Eric D. Knapp and Joel Thomas Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA and Other Industrial Control Systems* (2nd edn, Elsevier Inc 2015)

[17] Joel Brenner, *America the Vulnerable* (The Penguin Press 2011)

[18] See, for example, Kim Zetter, *Countdown to Zero Day* (1st edn, Broadway Books 2014) and Andy Greenberg, *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers* (1st edn, Doubleday 2019)

compromise operating systems and programs used by the general public, and secondly, once having been developed, these tools have proliferated. Proliferation can occur by reverse engineering of the tool once is has been deployed, or by theft of the tool from its developers,[19] and such proliferation will result in cyberattacks on the general public by cybercriminals who use these new and effective techniques.

These tools are unable to differentiate between what would be, when viewed through a Public International Law lens be a 'legitimate target' and a 'non-combatant' as the vulnerabilities which they exploit are present in the operating systems which are used by both groups, leaving both open to attack. This comparison with Public International Law is a heuristic device as firstly, Nation States who are engaging in cyberoffensive operations are not doing so under a declared state of war and secondly, it is not a settled question that cyberoffensive operations result in the use of 'force', which is a necessary for the action to fall under the sphere of International Humanitarian Law.[20] However, if we take a broad view of the term 'force', and assume that physical actions arising from cyberoffensive operations do constitute such a use of force, it is well established that under International Humanitarian Law, neither the civilian population nor individual civilians shall be the object of an attack.[21] The nature of the tools used in cyberoffensive operations are such that they would fail to stand up as valid under Public International Law due to their inability to be set to differentiate between civilian and non-civilian targets. This has been demonstrated by *NotPetya*, which was developed by a Russian hacker group which was affiliated with the GRU military intelligence agency,[22] and was released in retaliation against the killing of a Russian officer resulting in the crippling of corporate networks, hospitals, schools, local government authorities and global shipping, along with billions of dollars' worth of damage.[23] It can be argued, therefore, that when Nation States engage in cyberoffensive operations, they have a corresponding duty to increase the standard of cybersecurity among their own citizens in order to protect from the actions of other Nation States or the somewhat inevitable,[24] eventual use of their own tools against their citizens.

Maurer (2019) notes that when there is a militaristic approach to the discussion of cybersecurity on an international level, the discussants are constrained by the dual but incompatible desires to strengthen the cybersecurity of their own networks but weaken the networks of others.[25] Such a scenario may result in the development of a 'rules of engagement' type of agreement in how Nation States conduct cyberoperations but is fundamentally unsuited for the development of a safer online environment, a point

[19] See, for example, Scott Shane, Nicole Perlroth and David E. Sanger, 'Security Breach and Spilled Secrets have Shaken the N.S.A. to Its Core' *The New York Times* (New York, 12/11/2017) <https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html> accessed 01/06/2020

[20] Nils Melzer, 'Cyberwarfare and International Law' [2011] UNIDIR Resources: Ideas for Peace and Security 38.

[21] KJ Heller, '"One Hell of a Killing Machine": Signature Strikes and International Law' (2013) 11 Journal of International Criminal Justice 89.

[22] Greenberg (n 18)

[23] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' (2018) <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 23 March 2020

[24] Bruce Schneier has summarised this chain of events very succinctly: Today's top-secret programs become tomorrow's PhD theses and the next day's hacker tools. Bruce Schneier, *Data and Goliath* (W.W. Norton & Company 2015)

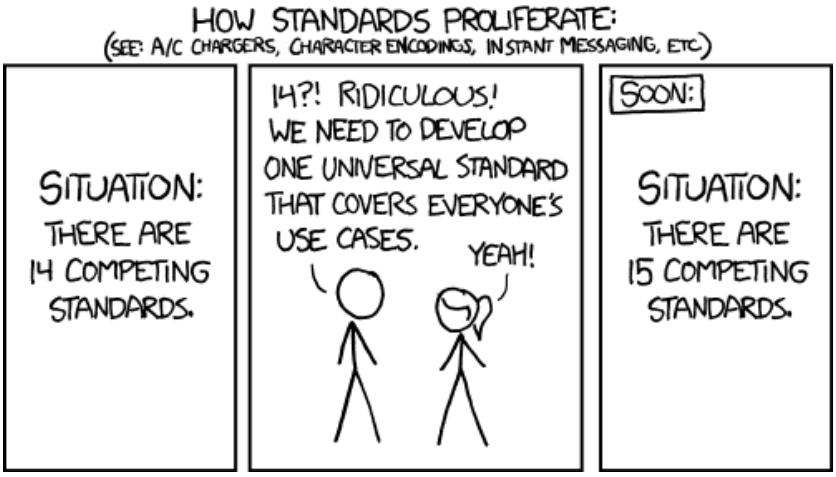
[25] Tim Maurer, 'A Dose of Realism: The Contestation and Politics of Cyber Norms' 2019 Hague J Rule Law 1

demonstrated by the fact that the National Security Agency in the United States of America was found to be 'hoarding' vulnerabilities to be used in future operations,[26] and the fact that such tools inevitable proliferate and fall into the hands of other actors, as outlined in this document.

It has also been suggested that a key stakeholder to a Nation State's cybersecurity policy is law enforcement,[27] as good cybersecurity practices can inhibit the ability of law enforcement to investigate crimes. This topic arises frequently in the discussion around encryption (of both data and internet access), and there have been repeated calls by the Law Enforcement bodies within Nation States for 'backdoors' and special access to the information systems of suspects and people of interest.[28]

It should be clear why there is a clear trichotomy between references to cybersecurity as a nation-state level initiative, cybersecurity from a law enforcement perspective and cybersecurity with regard to the practice of the implementation of the CIA triad, and that there is a corresponding set of competing incentives for Nation States when it comes to securing their own citizen's cybersecurity (and correspondingly, securing the systems of their targets) and passing legislation or taking illicit actions which allows for authorised actors within those states to attempt to compromise systems outside of their borders. It is the belief of the author that it is not possible to examine legislation which promotes the cybersecurity of a consumer without taking into account the negative implications such an action will have on other strategic cyberactions conducted by the Nation State.

4 Classifying Cybersecurity



Source: XKCD[29]

[26] Bruce Schneier, 'The NSA is Hoarding Vulnerabilities' (2016) <https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html> accessed 11/05/2020

[27] See, for example, Brenner (n 16) and Bruce Schneier, *Carry On: Sound Advice from Schneier on Security* (1st edn, John Wiley & Sons 2014) 291

[28] Amie Stepanovich and Michael Karanicolas, 'Why An Encryption Backdoor For Just the "Good Guys" Won't Work' (*Just Security*, 2018) <https://www.justsecurity.org/53316/criminalize-security-criminals-secure/> accessed 01/06/2020

[29] XKCD 'Standards'. Available at https://xkcd.com/927/ The image has been used with the consent of Randall Monroe

As outlined above, the term cybersecurity become too broad to maintain specific meaning and value. Therefore, the for the duration of this paper, four terms have been proposed as a framework to help ensure clarity, consistency and rigour when approaching the analysis.

Cybersecurity	Cybersecurity is taken to mean the actions taken to ensure the confidentiality, integrity and availability of an individual piece of software, Smart Device or computer.
Cyberhealth	'Health' has been chosen as the noun for this subset of actions, which relate to the active management of a network of information systems, as management of one's health is a continuous process, it is easy to conceptually assess health as being in a poor, medium or excellent health and furthermore, health management is a concept which is understand to have few absolutes – you can live a healthy lifestyle yet still get sick. Cybersecurity will still form a key element of cyberhealth, but it will be taken in consideration along with network security requirements, physical security requirements, information storage schema, etc. Heath was also chosen as it complements the principle that some cyberattacks are unpreventable and therefore no civil liability should attach following damages arising from the cyberattack.[30]
Cyberoffense	This term relates to the actions taken by nation states, which are seen as in their national interests, and principally relates to the attempt to weaken the cyberhealth of a third party sufficiently to breach the cybersecurity of their devices.
Cyberdefence	These are the policies which guide the practices which determine the cyberhealth of a network or computer infrastructure such as the NIST Framework, ISO 27001 requirements and various pieces of legislation.

5 The European Union's Approach to Cybersecurity

When examining the approach of the European Union to cybersecurity, the focus is on legislation drafted at the EU level, as opposed to the approach taken by individual member States. Notable legislation introduced by member states shall be discussed for comparative purposes where appropriate.

On the topic of cybersecurity, the EU is structurally quite different from other global powers in two key ways; firstly, as member states retain oversight of their own national security,[31] there is little scope for a cybersecurity policy to be developed from a militaristic framework, and secondly, as cybersecurity is not a core competency within the European Union, any cybersecurity policies must be derived from the foundation of other core competencies which can result in a lack of cohesion in its cybersecurity efforts. Article 114 of the TFEU, which allows for the enactment of legislation aimed at furthering the establishing and

[30] See Iain Nash, 'Cybersecurity in a Post Data Environment: Considerations on the Regulation of Code and the role of Producer and Consumer Liability in Smart Devices' 2020 Unpublished Working Paper <https://iainnash.ie/content/Cybersecurity_In_A_Post_Data_Environment.pdf>

[31] Paul Timmers, 'The European Union's cybersecurity industrial policy' 2019 3 J Cyber Policy 370

functioning of the internal market, is very frequently used for the implementation of cybersecurity related legislation.

However, just as the term cybersecurity is a suitcase word, cybersecurity within the European Union can be considered as something equivalent. When examining cybersecurity within the European Union, there are three primary components:

- Specific cybersecurity legislation
- Institutions with responsibility for their cybersecurity
- Legislation which imposes a requirement for cybersecurity on citizens, companies or institutions

The question of when the European Union began engaging with the topic of cybersecurity is not clear cut. Benediek and Maat (2019) state how the first engagement can be traced back to the completion of the internal market in 1985,[32] whereas a more tangible and specific example is the 2005 Framework Decision on attacks against information systems.[33] This Framework decision does not reference cybersecurity *per se*, but it is first piece of European legislation which defines and criminalises certain cybercrimes. The document itself makes reference to the need for increased coordination with regard to maintaining the security of information systems although it is silent when it comes to the nature of this security.

This piece of legislation arises directly as a result of an EU Commission Communication Document; Network and Information Security: Proposal for A European Policy Approach,[34] which summarises the EU Commission's view of cybersecurity in 2001. Interestingly, the document specifically calls out the CIA triad and the risks outlined, such as DDOS attacks are relevant for today. However, the focus of this concern is on the network, as opposed to the 'terminal devices' such as phones and computers. It is clear from the document that the Commission sees security as something which is controlled by the network, and therefore the responsibility of the network providers and the nation states in which they operate. Nowhere in the document is it suggested that a way to improve cybersecurity is reduce vulnerabilities in the network's nodes, nor legislate for a requirement to apply a minimum standard of cybersecurity for all users of a network. Thus, it is clear that the EU Commission took the viewpoint that the safety of internet users was something which was endogenous to the providers of the internet connection. This is a view which the author of this paper feels is incorrect.

The EU's Cybersecurity Act,[35] can be considered the cornerstone of the European Union's current approach to cybersecurity policy. The Act sets out a permanent mandate for the European Union Agency for Network and Information Security (ENISA) and introduces the concept of a cybersecurity framework for consumer products.

[32] Annegret Bendiek and Eva Pander Maat, 'The EU's Regulatory Approach to Cyber-security' 2019 Research Division EU <https://www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/WP_2019_Bendiek_Pander_Maat_EU_Approach_Cybersecurity.pdf>

[33] Decision 2005/222/JHA, repealed by Regulation 526/2013

[34] COM/2001/0298 final

[35] Regulation 2019/881

One immediate and key difference between the previous cybersecurity strategy (set out in 2013 Regulation[36]) and the 2019 Act is the introduction of the term 'cyber resilience'. There does not appear to be a clear definition of 'cyber resilience' published by the European Union and the term is another suitcase phrase which suggests elements such as being able to withstand and recover from a cyberattack. The term can generally be thought of to include have a multiplicity of controls within a system, which have a compensatory effect and can adapt to changes in the environment.[37] Resilience, when used by the European Union appears to refer to a system or network as opposed to an individual device and is an extension of the 'A' in the CIA triad. Systems which have successfully implemented the concept of 'resilience' into their design will be able to continue to provide their service during and after a cyberattack. Christou (2016) notes how many authors who discuss this topic describe the concept as returning to normal, following a critical incident,[38] and when assessing resilience in terms of the framework outlined in this document, it would fall under cyberhealth, with a focus on maintaining availability.

When assessing legislation within the terms of proposed framework, it is important to be able to differentiate between cybersecurity and cyberhealth. Within European Union Legislation, the demarcation is made clear by phraseology. When reference is made to cybersecurity as a matter of policy, the term 'cybersecurity' is often used, which refers to the concept of cyberhealth as outlined above. Cybersecurity, as defined in the framework, is indicated within EU legislation by reference to a specific reference to a requirement that the information system protects the 'confidentiality' and 'integrity' of the data. It is much less common within specific cybersecurity references to come across an 'availability' requirement, which is covered more as 'resilience' from a cyberhealth perspective.

Source	References to 'Cybersecurity'
Directives	4
Regulations	31

Source	References to 'Confidentiality' and 'Integrity'[39]
Directives	12
Regulations	64

It is very clear that the European Union takes a laissez-faire approach to how cybersecurity requirements are implemented by those who fall under the remit of such legislation. In general, there are no specific, or minimum requirements which software developers or firms have to adhere to, and there have been no cases taken by either the General Court or the European Court of Justice which have looked at specific cybersecurity requirements or failings.

[36] Regulation 526/2013

[37] See, for example the work by Ambore et al who discuss the design of a resilient mobile financial services system. Stephen Ambore and others, 'A resilient cybersecurity framework for Mobile Financial Services (MFS)' 2017 1 J Cyber Secur Technology 1

[38] George Christou, *Cybersecurity in the European Union* (Stuart Croft ed, 1st edn, Palgrave Macmillan 2016)

[39] The search strings used were: 'Confidentiality and integrity', 'integrity and confidentiality', 'confidentiality, integrity' and 'integrity, confidentiality'

In addition to the Cybersecurity Act, there are a number of other important pieces of legislation which can be considered as authoritative summaries of the European Union's approach to cybersecurity. Papantoniou (2017: 14) refers to the Network and Information Systems Directive,[40] as one of the most important pieces of legislation with regard to cyberhealth.[41] However, when viewed through the perspective of the framework outlined in this paper, the impact on safety can be seen as second order at best. The Directive requires that each Member State identify 'critical' information system infrastructure, and it requires each Member State to establish an expert authority who are to be notified by the operators of the essential services in the event of an incident regarding the security of their information system. However, there are no specific minimum cybersecurity requirements specified in the document and there is no legislated requirement or channel, although it is recommended,[42] for ENISA to support a Nation State following a cyberattack incident. The legislation is designed to create and support the coordination of cyberhealth policies applied by each Member State, but it is silent with regard to cybersecurity and does not create any framework which examines the safety of the endpoints (users) of such infrastructure.

However, there is some legislation which demonstrates how the European Union can outline very specific technical requirements with regard to cybersecurity. An example is Regulation 2016/799 which is outlines the regulatory requirements for vehicle Tachographs. Specific protocols are mandated to ensure that data related to a driver's records are confidential and accurate when being read and the annexes of the regulation include very detailed technical requirements for the cybersecurity of a tachograph reading.

The Second Payment Directive demonstrates how the European Union can be both detailed and prescriptive without being overly specific.[43] In the matter of Strong Customer Authentication, the Directive imposes specific cybersecurity requirements by requiring validation of payments to be based on something which the customer knows, something which the consumer has and something which the consumer is. This provides robust security as a breach of a single element will not allow the third party to compromise the consumer's authentication details and yet the specifics of the legislation are up to the Member States and is an excellent example of how to legislate for both cybersecurity and cyberhealth.

Thus, it appears to be a conscious decision by the drafters of European legislation to generally vague when it comes to cybersecurity specifics and to ignore the development of legislation which is aimed at directly increasing both the cybersecurity and cyberhealth of commonly used consumer information systems. This point is developed further, when 'missing' legislation is analysed.

5.1 Breach Notifications

There are twenty-one references to 'personal data breach' within the text of European Union Directives and Regulations, although in most examples, the reference is a mirror of

[40] Directive 2016/1148/EU

[41] Margarite Papantoniou, 'Economic Fraud Crimes on the Internet: Development of New 'Weapons' and Strategies to Annihilate the Danger' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law: Regulation and Enforcement* (1st edn, Springer International Publishing 2017)

[42] Directive 2016/1148/EU, Recital 4

[43] Directive 2015/2366

the text as set out in the General Data Protection Legislation,[44] although exceptions are the Europol Regulation which doesn't impose a 72 hour requirement to report the data breach to the supervisory authority and instead only requires notification without 'undue delay',[45] and regulations which, in addition to the GDPR requirements, mandate that other bodies or authorities are notified following a personal data breach.

It is interesting to note that the requirements as set out in Regulation 2013/611, which outlines the breach notification requirements for public electronic communications services. The regulation required that the supervisory authority is notified within 24 hours of the breach, where feasible and they were required to notify the data subject *where the breach is likely to adversely affect the personal data or privacy of a subscriber … without undue delay*.[46] This is contrasted with the GDPR requirements which require notification to the supervisory authority within 72 hours, and notification to the data subject is required only if '*there is a high risk to the rights and freedoms … [of] the data subject*, and notification is only required if the data which was breached was unencrypted.[47]

During the course of this analysis, no pieces of legislation have been found which outline the requirement to notify the data subject of a breach to their data, without also requiring that such data was to be protected by cybersecurity methodologies, although there was no guidance provided as to what form the cybersercurity methodologies should take.

5.2 'Missing' Legislation

The Botnet Directive,[48] which criminalises the use of large number of coordinated devices to attack an information system refers to the importance having secure computer systems, and calls out the threat caused by such attacks to critical infrastructure, but is completely silent on the topic of cybersecurity even though the risks of such attacks are outlined in the legislation. This is particularly relevant for cybersecurity policy for consumers as botnets are frequently built on compromised smart devices which exploit insecure programming, a lack of security updates and the fact that such devices are commonly used on an 'unattended' basis when compared to traditional computers.[49]

A second example of recent legislation which has, surprisingly, no mention of either cybersecurity or cyberhealth is the 2019 Modernisation of the Consumer Protection Directive.[50] This directive draws heavily on the foundations laid in the 2019 Supply of Digital Content and Digital Services Directive,[51] and the 2011 Consumer Rights Directive.[52] Within these three directives, which form the basis of granting a consumer their rights when entering into an agreement to purchase an information system relating to either a product or a service, there is neither a requirement for the information system to have cybersecurity

[44] Regulation 2016/679
[45] Regulation 2016/794, Art 34
[46] Regulation 2013/611, Art 3
[47] Regulation 2016/679, Art 34
[48] Directive 2013/40/EU
[49] See, for example, Natalija Vlajic and Daiwei Zhou, 'IoT as a Land of Opportunity for DDoS Hackers' 2018 51 Computer 26 and Constantinos Kolias and others, 'DDoS in the IoT: Mirai and Other Botnets' 2017 50 Computer 80
[50] Directive 2019/2161
[51] Directive 2019/770
[52] Directive 2011/83/EU

elements nor is there a requirement for the developer or manufacturer to have a cyberhealth policy to protect the consumer from exploits, a point also made by McGillivrary (2017).[53]

5.3 Conclusion

In conclusion, the European Union approach to cybersecurity appears to be comprised of four distinct layers. The top layer refers to specific requirements for critical network infrastructure (as defined by each member state) within the European Union. Each member State is required to draft a cybersecurity plan and engage with the operators of the infrastructure. Coordination (of sorts) between member states is handled through ENISA, who can engage with the local CSIRT established in each member state.

It is the view of the author that the top layer, although a positive and welcome step, is more aspirational than practical. This view is based on two points; the first being that although the EU has developed an expert cybersecurity body, the legislation only mandates interaction as a response to a cyberattack and does not require an assessment of the efficacy of each member state's preparedness. Within the legislation itself, there is no reference to minimum standards and there are no penalties for member states who either fail to engage with the exercise on a serious basis or who fall short in their execution.[54]

The middle layers relate to the mandating of EU institutions and bodies to engage in cybersecurity, as well as funding research and development for cybersecurity. The European Commission has noted that between 2014 and 2016, €160 million was invested in cybersecurity research and innovation projects through the Horizon 2020 Programme.[55] Other areas of investment have been highlighted by the Commission, however their focus has been on the cybersecurity of large infrastructure projects, even though the Commission itself has reported that individual citizens are growing more afraid of becoming victims of cybercrime conducted through their digital and smart devices.[56] The inclusion of cyberhealth related language in recent legislation which refers to EU institution and bodies is welcome, even though no guidance is given to these bodies as to what minimum level of cyberhealth should be applied.

Finally, the bottom layer relates to consumer products. Up until the Cybersecurity Act, the EU has been quiet with regard to the cybersecurity of such products, but the Act outlines the concept of a cybersecurity framework for consumer products. It is clear there is neither appetite within the Union to engage in the regulation of cybersecurity nor to set a minimum standard for regulation as, from the analysis of 'Missing Legislation', the EU is quiet on the subject in its key pieces of consumer protection legislation. There has been some specific attempts to remedy this by bodies which are connected to the European Union. The European Telecommunications Standards Institute (ETSI) is a body recognised by the European Commission and is responsible for the development of ICT standards. The ETSI

[53] Kevin McGillivray, 'A right too far? Requiring cloud service providers to deliver adequate data security to consumers' 2017 25 Int J Law Information Technology 1

[54] It should be noted however, that 'falling short' is something which is very difficult to define with sufficient precision to allow for an action because there are no minimum standards nor required expert oversight

[55] The European Commission, 'COM(2017) 228 Final' *Mid-Term Review on the Implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All* (2017) 37

[56] *Ibid, p 39*

have in 2019 created a high-level set of technical standards for consumer IoT devices,[57] which themselves appear to be similar to the conclusions of the United Kingdom's Code of Practice for Consumer IoT Security.[58] While it is very welcome to see such publications, they are non-binding on manufacturers and it is disappointing to see that both Codes only 'recommend' that consumer IoT devices should encompass a mechanism to allow for post-sale security updates. At the time of writing, there are no communications from the European Commission nor pieces of legislation which reference the ETSI standards.

A European Commission report, which was prepared by cybersecurity experts,[59] also suggested that economic and legal incentives are introduced to encourage both disclosure of technical vulnerabilities and responsible disclosure policies. It is interesting to note that although this report was cited in the Mid Term Review of the Digital Market Strategy,[60] the focus of the citation was on increased cooperation between Member States, and the consumer level suggestions outlined were not mentioned and there does not appear to be any EU Commission documents,[61] which discuss the rolling of out of minimum standards for the cybersecurity measures required for consumer devices.

However, although EU cybersecurity legislation as it stands will have very little first order impact on the safety of consumers, there are still positives. The GDPR specifically mandates that any data processor or controller undertake cybersecurity activities (although the specifics are undefined) to protect the CIA of a data subject, and the EU in recent regulations has required its own institutions to undertake cybersecurity activities. It can be argued that the EU has begun, with the exception of consumer products, to introduce a cybersecurity framework and that the groundwork has been set for the rolling out of minimum standards of cybersecurity, an outcome which is discussed in a summary of the European Union's Digital Market Strategy,[62] suggesting that although the European Union lacks a specific competency for the imposition of specific cybersecurity requirements, it is a safe assumption that such an outcome is on the Digital Single Market roadmap.

6 The United States of America's approach to Cybersecurity

When assessing cybersecurity related legislation in America, the focus is on Federal law which is applicable in all states, although prominent state laws (such as those enacted in New York and California) will also be discussed. This approach is equivalent to that taken in the analysis of the European Union legislation.

One key ideological difference between European and American approaches to legislation and regulation is that in Europe, regulation is frequently drafted expressly to protect citizens from the risks of technological development while in the USA, regulation has been drafted within the context that there is a persistent race for technological progress,[63] which can

[57] ETSI TS 103 645 V1.1.1
[58] Code of Practice for IoT Security, 2018, Department for Digital, Culture, Media and Sport
[59] The European Commission, 'Scientific Opinion No. 2/2017' *Cybersecurity in the European Digital Single Market* (High Level Group of Scientific Advisors, 2017)
[60] Commission, *Mid-Term Review on the Implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All*
[61] As opposed to documents which were published by the Committee but prepared by external parties
[62] COM(2015) 192

make it more challenging to enact regulations which lead to direct costs for producers but have only indirect benefits for consumers.

Cybersecurity legislation within the United State is both opaque and complicated as there is no singular piece of legislation within the United States which provides a Federal cybersecurity framework, instead there a number of notable pieces of distinct legislation, enacted over the past forty years, which provide the legislative basis for cybersecurity within the United States. *The Computer Act of 1987*,[64] has a direct impact on the cyberhealth of Federal computer systems as it assigned to the National Institute of Standards and Technology (NIST) the responsibility to develop minimum standards for cybersecurity, as well as mandating cybersecurity training for Federal employees who use systems which contain sensitive data. These standards are not required to be used by non-Federal computer systems. *The 1995 Paperwork Reduction Act* requires that the Office of Management and Budget establish the Office of Information and Regulatory affairs which has responsibility for, inter alia, the drafting of cyberhealth policies.[65] *The Homeland Security Act of 2002*,[66] requires that the Department of Homeland Security manage the cybersecurity of some critical infrastructure systems. *The Cyber Security Research and Development Act of 2002*,[67] establishes responsibilities for both the National Science Foundation and NIST to research the topic of cyberhealth and cybersecurity. The *Federal Information Management Security Act of 2002*,[68] introduces the responsibility for all heads of Federal Agencies to reduce cybersecurity risks to an acceptable level in a cost effective manner. Finally, the *Financial Modernisation Act of 1999*,[69] otherwise known as the Graham-Leach-Bliley Act has some cybersecurity requirements in that companies who fall under its auspices are required to create an information security plan and outline to their customers how their data is being handled, notify customers in the event of a data breach and provide out-opt options for customers who don't wish for their data to be shared with third parties. The *Health Information Portability and Accountability Act of 1996* (HIPAA),[70] is a federal law which has both a direct and indirect effect on the security of an individual's devices. The law was drafted to set out a clear set of standards to allow for health related information to be shared between healthcare providers and other medical companies. The indirect effect is the requirements that it places on medical service providers, but the direct effect is on any medical devices which a consumer may own.

From the above, it is clear that when it comes to Federal cyberhealth requirements, responsibility has been handed out to many departments. There is a lack of cohesive legislation, and accordingly, there is a lack of clarity when it comes to accountability for cybersecurity within the Federal government as there are many overlapping departments who are responsible for very similar aspects of cyberhealth. Furthermore, this legislation is

[63] Araz Taeihagh and Hazel Si Min Lim, 'Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks' 2019 39 Transport Rev 103, 7
[64] Public Law 100-235 (1988)
[65] Public Law 104-13 (1995), Section 3504
[66] Public Law 107-296 (2002)
[67] Public Law 107-355 (2002)
[68] Public Law 107-347 (2002)
[69] Public Law 106-102 (1999)
[70] Public Law 104-191 (1996)

focused on the cyberhealth of Federal departments and has no impact on the direct cybersecurity safety for a consumer.

On a State legislative level, the Department of Financial Services in New York State in 2017 introduced legislation which required certain financial services companies and banks to develop and implement a robust cybersecurity programme with associated policies and audit trials which is based on the standards developed by both NIST and the ISO.[71] Although this law was introduced to "… ensure the safety and soundness of the institution and protect its customers",[72] it does not have a direct effect upon the safety or cyberhealth of equipment used by consumers, but should protect their financial interests by requiring their bank to have a cyberhealth practices in place. The legislation itself is an excellent example of how to regulate for cybersecurity; some specifics (such as use of encryption and multifactor authentication) and the need to either hire or contact qualified cybersecurity experts are set out explicitly along with the requirement to implement both cyberhealth policies and practices, however, the specific way in which the business implements remains a business decision.

6.1 Recent Legislation

Having reviewed the recent cybersecurity legislation introduced by the European Union, a similar exercise has been conducted for legislation enacted by the Federal Government. The 115th Congress, which spanned from 3 January 2017 (the final weeks of Barrack Obama's Presidency) until 3 January 2019 passed 10 pieces of legislation which were enacted by President Trump and were directly or tangentially related to cybersecurity.[73] In addition to these enacted bills, 48 more bills were passed by at least one house but were not voted in the second. In total, 226 bills were proposed during the 115th Congress, which was the highest number of any congress,[74] and demonstrates how the topic has grown in stature from the perspective of the legislature.

The 116th Congress, which is at the time of writing in session has to date passed 12 pieces of legislation which contain the term cybersecurity. The majority of these bills relate to cybersecurity appropriations, although one bill examines the cybersecurity implications of a cyberattack on the nation's health systems and the second on an attack on the IRS. Therefore, it is clear that cybersecurity, although growing in frequency as a topic enacted within legislation, is not referred to as frequently as it is in the European Union. During the period of review, there were no pieces of legislation which could be considered to directly increase the security of a consumer's device.

6.2 Consumer Regulation

From a consumer perspective, this result is somewhat replicated. The Federal Trade Commission (FTC) is the de facto regulator of consumer products and this includes cybersecurity. However, the FTC does not regulate companies who provide internet connectivity services, as this falls under the auspices of the Federal Communications

[71] 23 NYCRR 500
[72] Ibid, Section 500.00
[73] Ishan Mehta and Jayati Dev, 'Taking Action on Cyber Enforcement: Assessing US Legislative Progress in the 115th Congress' 2019 Third Way
[74] *ibid*

Commission (FCC). Furthermore, when it comes to consumer interaction with financial services, as this is regulated by the Federal Reserve Board.

The FCC has an indirect impact on consumer safety through its regulation of ISPs, but the Commission does not have oversight of the endpoints on the network. Simpson (2017), in an FCC white paper, outlines the security principles and objectives which are imposed on ISPs operating in the United States,[75] but these can only be seen as second-order effects on consumer safety.

The FTC's role in the regulation of consumer cybersecurity stems from a law passed in 1914,[76] which prohibits a company from engaging in 'unfair or deceptive' practices.[77] This act clearly pre-dates the concept of cybersecurity as well as the concept of computing itself, but the FTC began using this clause in 2002 and for ten years all enforcement actions issued were uncontested by the companies in question.[78] The first legal challenge to the FTC was brought by Wyndham Worldwide Corporation in 2012, a hotel company who had stored personal data associated with their customers, and this data was subsequently hacked by a third party. Wyndham challenged the enforcement order issued by the FTC in Court, where it was held that Section 5 of the FTC Act did enable the FTC to regulate the cybersecurity of companies who fall under its remit.

The extent of FTC regulation can be seen from the case of FTC v. LabMD Inc.[79] LabMD was a medical company which provided cancer diagnostic services. A member of the billing team had installed LimeWire, which was a peer-to-peer file sharing tool and in the process of the installation, had made the entire 'My Documents' folder on the computer shareable. A third party company, called Tiversa, was able to access the folders shared by the LabMD employee and access a billing file which contained patient details. Tiversa, having attempted to sell LabMD cybersecurity services, then reported LabMD to the FTC.[80]

It appears that the FTC is attempting to set the standard of cybersecurity through the same methodology that it used with regard to data protection. Solove and Hartzog (2013) note how the FTC, through its frequent use of non-litigated enforcement orders have actually become the primary source of data protection standards within the United States,[81] and therefore their private enforcement actions (which are public) have become, in effect, case law on the topic. Hoofnagle (2017) notes how the FTC are developing their own standards which are being applied to companies and used to impose liability when their code is found to be insecure.[82]

---

[75]David Simpson, 'Cybersecurity Risk Reduction' (Federal Communications Commission 2017) FCC White Paper.
[76] 15 U.S.C. §§ 41-58, as amended
[77] *ibid*, Section 5
[78] William R. Denny, 'Cyber Center: Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act' 2016 Business Law Today 1
[79] No. 16-16270 (2018)
[80] For a comprehensive of the type of cybersecurity services offered by Tiversa, see Raffi Khatchadourian, 'A Cybersecurity Firm's Sharp Rise and Stunning Collapse ' *The New Yorker* (New York, 28/10/2019) <https://www.newyorker.com/magazine/2019/11/04/a-cybersecurity-firms-sharp-rise-and-stunning-collapse> accessed 11 July 2020
[81]Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' [2013] SSRN Electronic Journal <http://www.ssrn.com/abstract=2312913> accessed 10 August 2020.

The FTC found that the cyberhealth activities of LabMD were insufficient and imposed a new cyberhealth regime. This was challenged by LabMD and the FTC requirements were eventually overturned in court. The court did not overturn the FTC requirements on the basis that it lacked the competency to regulate cybersecurity, but rather that the FTC did not demonstrate actions which LabMD were performing which were specifically endangering consumers. Instead, the FTC were imposing a new cyberhealth regime which court determined was unenforceable. It was made clear in the judgement that if the FTC had focused on the specific LimeWire incident, and limited its response to a prevention of the installation of further unauthorised programs, then the outcome of the judgement would have been different.[83]

It is clear from the decision in FTC v LabMD that the judiciary are wary of the complexity associated with enforcing unclear cybersecurity guidelines. Indeed, it was made clear by the court that the software principles as outlined by the FTC are themselves too vague to be enforceable, and that the FTC have been taking actions to attempt to remedy this.[84] However, the somewhat worrying conclusion is that when it comes to cyberhealth, specific and focused cybersecurity requirements may be enforceable by the judiciary, but larger scale defects which require enforced cyberhealth intervention will not be.

6.3 Conclusion

When comparing the approach to both cyberhealth in general, and specifically the cybersecurity of an individual taken by the European Union and the United States of America, two apparent mutually exclusive points are apparent. The first is that there appears to be a more concentrated and focused effort within the European Union to incorporate at least the nomenclature of cyberhealth into legislation, and also to create a, relatively speaking, simplified cyberhealth reporting and information sharing structure among Member States. When compared to the USA, there is a much larger number of pieces of legislation passed which refer to cyberhealth, and there has been a clear attempt to coordinate cybersecurity activities. Within both jurisdictions, however, the focus upon cyberhealth legislation has been within governmental departments as opposed to protecting the devices used by their respective citizens.

However, the FTC in the United States of America has shown a much greater appetite to engage with companies who have demonstrably failed in their cyberhealth approaches and who have caused damage to consumer's data. Furthermore, the FTC has issued guidance to manufacturers of Smart Devices,[85] and the recent settlement in *Tapplock*,[86] demonstrates how they are willing to pursue companies who fail to follow cybersecurity principles. Although in the Tapplock example, the complaint was centred around the Tapplock services as opposed to the IoT device itself. Therefore, as things stand, it is clear that within the United States, although consumer have less specific cyberhealth legislation which grants

[82]Chris Hoofnagle, 'FTC Cybersecurity and Surveillance' in David C Gray and Stephen E Henderson (eds), *The Cambridge handbook of surveillance law* (Cambridge University Press 2017).
[83] FTC v LabMD Inc, No 16-16270 (2018), page 14
[84] Randy Milch and Sam Bieler, 'A New Decade and New Cybersecurity Orders at the FTC' *Lawfare* (29/01/2020) <https://www.lawfareblog.com/new-decade-and-new-cybersecurity-orders-ftc> accessed 11 July 2020
[85] FTC Staff Report, *Internet of Things: Privacy and Security in a Connected World* (2015)
[86] Tapplock Inc, File Number 192 3011

them protections, there is an active regulator who will take action against companies who fail to take cybersecurity seriously. This is caveated somewhat by the result in the *LabMD* case and the lack of a specific minimum standard of cybersecurity, but it highlights the willingness of a regulator to enforce minimum standards of cybersecurity.

In general though, it can be said that the majority of legislation passed within the United States that relates to the topic of cybersecurity will have an indirect effect on most consumers and will have little impact on their online safety.

7 Cybersecurity in Other Countries

Huang and Li (2018) outline the approach taken by Taiwan with regard to Information Security, a phrase which is used interchangeably with cybersecurity.[87] The approach to developing a robust state of cyberhealth in the country can be seen somewhat of a hybrid of the European and American approaches. Overall responsibility for the subject has been given to the military and indeed the subject is seen mostly as a form of cyberdefense, especially given the antagonistic relationship between Taiwan and China. Militaristic control will most likely result in the same conflicts of interest between cyberoffence and cyberdefence as has been outlined in this paper. Secondly, the government has begun to invest in the skills gap in the cybersecurity industry. Given the context of the control of the cyberhealth program, such an investment will not necessarily translate into directly safer devices used by consumers, although it should lead to an indirect effect as the services used by consumer should have more robust cyberhealth as a consequence of increased local skill. Finally, the Taiwanese government has followed a path of identifying critical infrastructure targets and mandating that the relevant businesses who operate them have sufficient cyberhealth.

While the direct investment in areas designed to upskill the local cybersecurity talent is a welcome policy, and while it does appear to be relatively more focused and larger than similar policies in either the United States or in Europe, there appears to be little in the approach taken by Taiwan which will directly improve the cybersecurity for consumer users.

Kshetri (2018) provides an excellent summary of the state of cybersecurity in Africa, but worryingly outlines how there has been a lack of cybersecurity development, which has resulted in a weakened form of cyberhealth in private and public Information Systems.[88] These findings are also replicated in work by Kabanda et al. (2018).[89] The establishment of a robust cybersecurity framework in Africa is a task which is made more complicated by a lack of a regional body who could coordinate such actions. Furthermore, it is generally noted that Africa has a problem with cybercrime which arises due to a lack of both relevant legislation in some countries to prohibit what would elsewhere be illegal acts and enforcement in countries which have enacted such legislation.[90] Given this context, it is

[87]Hsini Huang and Tien-Shen Li, 'A Centralised Cybersecurity Strategy for Taiwan' (2018) 3 Journal of Cyber Policy 1.
[88]Nir Kshetri, 'Cybercrime and Cybersecurity in Africa' (2019) 22 Journal of Global Information Technology Management 1.
[89]Salah Kabanda, Maureen Tanner and Cameron Kent, 'Exploring SME Cybersecurity Practices in Developing Countries' (2018) 28 Journal of Organizational Computing and Electronic Commerce 269.

perhaps understandable that cybersecurity is seen as a luxury as opposed to a necessity.[91] However, it is the view of the author of this paper that given that there are estimates of between one to two billion internet connected endpoints within the continent and the fact that unlike other regions such as Asian or India where local technologies are used in preference to international operating systems and applications, if there is a uplift in both cybersecurity and cyberhealth practices in smart phones and smart devices, such practices will be applied in Africa.

8 Conclusion

From this document, it should be now clear that while some countries have taken legislative measures to protect their critical infrastructure and government departments, there has been little in the way of enacted legislation which enshrines a solid cybersecurity grounding for a consumer's device nor is there legislation which requires a minimum standard of cyberhealth, which results in the conclusion that there has been little in the way of legislation which has improved safety for consumer users.

Part of this outcome can be seen as the consequence of the incompatibility of a Nation State both protecting consumer devices and engagement in covert cybersecurity actions, as discussed in this document earlier, can be highlighted by the recent expose by Kim Zetter that in 2018 President Trump signed a presidential finding which allowed the Central Intelligence Agency to engage in, *inter alia*, actions such as 'hack and dumps', where private information relating to foreign targets is obtained and released to interested third parties, and cyberoffensive operations against critical infrastructure targets.[92] The extent to which the power has been used, and indeed, the discussion as to whether such a finding was warranted has been discussed elsewhere,[93] and fall outside of the scope of this article, however, the fundamental dichotomy between actions taken to protect citizens from a cyberattack and the ability to cause cyberoffensive and physical disruption to another countries citizens is a large hurdle to be overcome before meaningful cybersecurity legislation can be passed.

In addition to this, it is important to note the evolution of how both cybersecurity in particular, and software liability in general has arisen. The European Union, when first beginning to discuss cybersecurity, took the view that as the networks were controlled by a small number of ISPs, they would be responsible for the security of the network. As a result, when legislators began to formulate cyberhealth policy, the endpoints of the network (the consumer products) were seen as both exogenous to the fundamental security of the network and out-of-scope for regulation. This core centric view remains today (and with good reason) in the context of 5G security, where cybersecurity threats to the infrastructure which powers the 5G network has resulted in the European Union creating a 'toolbox' and a

[90]Felix E Eboibi, 'Concerns of Cyber Criminality in South Africa, Ghana, Ethiopia and Nigeria: Rethinking Cybercrime Policy Implementation and Institutional Accountability' (2020) 46 Commonwealth Law Bulletin 78.
[91]Kshetri (n 84).
[92]Kim Zetter and others, 'Exclusive: Secret Trump Order Gives CIA More Powers to Launch Cyberattacks' [2020] *Yahoo! News*.
[93]See, for example, Robert Chesney, 'The CIA, Covert Action and Operations in Cyberspace' *Lawfare* (15 July 2020) https://www.lawfareblog.com/cia-covert-action-and-operations-cyberspace

tripartite framework between Member States, the Commission and ENISA.[94] There is an equivalent exercise taking place within the United States.[95]

This can in part be understood when viewed through the context of regulation at this time, as at the time of the 'dot com boom', the internet and on-line activity had not become the dominant tool which it is now as more traditional telecommunications tools were still used to communicate, and within the provision of the internet to consumers, there were two dominant but very diverse cultures; the 'netheads' and the 'bellheads'.[96] The bellheads represented the ISPs, whose school of thought was based on the establishment of telecommunications networks from the 1960s, while the netheads were focused on applications which used the network. Since the advent of telecommunications, regulatory and security focus has been on network itself, as that is where the threats lay. It was the 'bellheads' who faced regulatory scrutiny while the 'netheads' were able to escape such oversight and prevent the equivalent of telecommunications oversight in the form of internet governance.

However, since the advent of 3G which enabled mobile devices to communicate with the internet at speeds which were sufficient to support browsing via mobile devices,[97] the risk profile has altered to now include threats to the endpoint of the network as we have become dependent on data, which is accessed through the network. Therefore, the risks have extended from protecting the critical infrastructure which is the backbone of such access, and as should be clear from this paper, reasonably well covered from a legislative perspective to also including availability of such data and the integrity of the data, which requires specific cyberhealth legislation which is unfortunately lacking.

This outcome, although unwelcome is not that unexpected. The legislative approach to the applications developed by the 'netheads' has potentially fallen victim to what Jared Diamond calls 'creeping normality' or 'landscape amnesia'; where change a certain change in an environment is regular and gradual.[98] This effects how the change is viewed, as it compared to recent events and appears reasonably static. Consequently, the total effect of this change over a number of years can be dramatic yet remaining invisible to the participants. This hypothesis may seem to conflict with the standard view of technological progress, which is fast, spectacular and unrelenting, but although counter-intuitive, appears to hold when applied to an analysis of software related legislation.

From an American context, the first cases which examined whether software should be released 'error free' were taken in the 1980s, and the software in question would be unrecognisable to the current form.[99] Scott (2008) also makes reference to the fact that

[94]https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1378

[95]Donald Trump, 'National Strategy to Secure 5G of the United States of America' <https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf> accessed 27 July 2020.

[96]Rob Frieden, 'Revenge of the Bellheads: How the Netheads Lost Control of the Internet' [2002] Telecommunications Policy 20.

[97]Bruce Schneier has identified this inflection point as c. 2007 when the Iphone became widely available, ushering in the era of 'Internet+'. Click Here to Kill Everybody (WW Norton & Company 2018).

[98]Jared Diamond, *Collapse: How Societies Choose to Fail or Succeed* (1st edn, Penguin 2005) 426.

[99]Janice C Sipior, Burke T Ward and William P Wagner, 'The Increasing Threat of Legal Liability for Software Developers': (1998) 11 Information Resources Management Journal 25.

software in this era was actually shipped and was distributed via physical media.[100] It is now common to download software directly, and for many years there was a hybrid model whereby the core code would be shipped via a physical medium, but updates (which were much smaller packages) could be downloaded from the internet. This meant, that at the time of the formative years of legislation surrounding software, decisions regarding issues such as product liability were made at a time when the practicalities of correcting errors were similar to those of a product recall. Furthermore, as noted by Scott, in the 1980s and 1990s there was a much clearer distinction between software and security software – security was handled by a distinct program, usually developed by a third party.[101] These factors, combined with the ability of the 'netheads' during the time to avoid regulation and the focus of regulators on the infrastructure allowed a laissez-faire environment to develop which has little to little in the way of consequence for the creation of insecure software. Bruce Schneier has been making a similar point for almost the past two decades; the market does not reward companies who ship slower but ship more secure code, and there is very little consequence for producing insecure and lower quality software.[102]

In addition to this, it has been noted by the courts that part of their reluctance to get involved in the question of cybersecurity is that there is no test which can applied, and that the question is quite open ended.[103] The principles as outlined in Nash (2020),[104] are a potential solution to this problem.

This again highlights how the European Union, which does not have a competency for military or cyberwarfare actions, is the most appropriate choice for a global entity to begin to legislate specifically for the cybersecurity of a consumer's device, especially as Europe is the single largest market bloc in world. However, before this is possible, and in order to ensure that the term cybersecurity does not remain a 'suitcase word' there must be a clear set of minimum standards of cybersecurity for consumer devices as outlined in Nash (2020),[105] Brenner (2004),[106] and in Rustad (2005).[107]

---

[100]Michael D Scott, 'Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?' (2008) 2 Maryland Law Review 61.
[101]ibid.
[102]See for example, Bruce Schneier, 'Testimony before the Subcommittee on Cybersecurity, Science, and Research and Development' (*Schneier on Security*, 25 June 2003) <https://www.schneier.com/essays/archives/2003/06/testimony_before_the.html> accessed 23 July 2020. Bruce Schneier, 'Cryptogram' (*Schneier on Security*, 15 November 2004) <https://www.schneier.com/crypto-gram/archives/2004/1115.html>.,Bruce Schneier, 'Liabilities and Software Vulnerabilities' (*Schneier on Security*, 20 October 2005) <https://www.schneier.com/blog/archives/2005/10/liabilities_and.html> accessed 23 July 2020. and Bruce Schneier, 'Security and the Internet of Things' (*Schneier on Security*, 2 January 2017) <https://www.schneier.com/blog/archives/2017/02/security_and_th.html> accessed 23 July 2020.
[103]Dominic Callaghan and Carol O'Sullivan, 'Who Should Bear the Cost of Software Bugs?' (2005) 21 Computer Law & Security Review 56.
[104]Nash (n 30)
[105]ibid.
[106]Susan W Brenner, 'Towards a Criminal Law for Cyberspace: Product Liability and Other Issues' (2004) 5 Journal of Technology Law and Policy.
[107]Michael L Rustad and Thomas H Koenig, 'The Tort of Negligent Enablement of Cybercrime' (2005) 20 Berkeley Technology Law Journal.

Instrument	Reference	Name	CELEX
Directive	2019/944	Common rules for the internal market for electricity and amending Directive 2012/27/EU	32019L0944
Directive	2018/844	Amending Directive 2010/31/EU on the energy performance of buildings and Directive 2012/27/EU on energy efficiency	32018L0844
Directive	2018/2002	Amending Directive 2012/27/EU on energy efficiency	32018L2002
Directive	2016/1148	Concerning measures of a high common level of security of network and information systems across the Union	32016L1148
Regulation	513/2014	Establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management and repealing Council Decision 2007/125/JHA	32014R0513
Regulation	2019/943	On the internal marketing for electricity	32019R0943
Regulation	1291/2013	Establishing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC	32013R1291
Regulation	230/2014	Establishing an instrument contributing to stability and peace	32014R0230
Regulation	2019/2144	Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166	32019R2144
Regulation	2017/1369	Setting a framework for energy labelling and repealing Directive 2010/30/EU	32017R1369
Regulation	283/2014	On guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision no 1336/97/EC	32014R0283
Regulation	2019/881	On ENISA (the European Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)	32019R0881
Regulation	2019/1150	On promoting fairness and transparency for business users of online intermediation services	32019R1150
Regulation	2019/941	On risk-preparedness in the electricity sector and repealing Directive 2005/89/EC	32019R0941
Regulation	2019/517	On the implementation and functioning of the .eu top-level domain name and amending and repealing Regulation (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004	32019R0517
Regulation	2019/452	Establishing a framework for the screening of Foreign Direct Investments into the Union	32019R0452
Regulation	2018/1807	On a framework for the free flow of non-personal data in the European Union	32018R1807
Regulation	2018/1092	Establishing the European Defence Industrial Development Programme aiming at supporting the competitiveness and innovation capacity of the Union's defence industry	32018R1092
Regulation	2019/2175	amending Regulation (EU) No 1093/2010 establishing a European Supervisory Authority (European Banking Authority), Regulation (EU) No 1094/2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority), Regulation (EU) No 1095/2010 establishing a European Supervisory Authority (European Securities and Markets Authority), Regulation (EU) No 600/2014 on markets in financial instruments, Regulation (EU) 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds, and Regulation (EU) 2015/847 on information accompanying transfers of funds	
Regulation	526/2013	Concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation No 460/2004	32013R0526
Regulation	2019/2199	Amending Council Regulation (EC) No 428/2009 setting up a regime for the control of exports, transfer, brokering and transit of dual-use items	32019R2199
Regulation	184/2014	laying down pursuant to Regulation (EU) No 1303/2013 of the European Parliament and of the Council laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund and laying down general provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund and the European Maritime and Fisheries Fund, the terms and conditions applicable to the electronic data exchange system between the Member States and the Commission and adopting pursuant to Regulation (EU) No 1299/2013 of the European Parliament and of the Council on specific provisions for the support from the European Regional Development Fund to the European territorial cooperation goal, the nomenclature of the categories of intervention for support from the European Regional Development Fund under the European territorial cooperation goal	32018R1139
Regulation	2017/373	Laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and	32017R0373

		their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011	
Regulation	2019/947	On the rules and procedures for the operation of unmanned aircraft	32019R0947
Regulation	2019/411	Supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards setting technical requirements on development, operation and maintenance of the electronic central register within the field of payment services and on access to the information contained therein.	32019R0411
Regulation	215/2014	laying down rules for implementing Regulation (EU) No 1303/2013 of the European Parliament and of the Council laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund and laying down general provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund and the European Maritime and Fisheries Fund with regard to methodologies for climate change support, the determination of milestones and targets in the performance framework and the nomenclature of categories of intervention for the European Structural and Investment Funds	3201R2015
Regulation	2016/1377	Laying down common requirements for service providers and oversight in air traffic management/air navigation services and other air traffic management network functions, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011 and (EU) No 1035/2011 and amending Regulation (EU) No 677/2011	32016R1377
Regulation	2019/1583	Amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures	32019R1583
Regulation	2019/876	Amending Regulation (EU) No 575/2013 as regards the leverage ratio, the net stable funding ratio, requirements for own funds and eligible liabilities, counterparty credit risk, market risk, exposures to central counterparties, exposure to collective investment undertakings, large exposures, reporting and disclosure requirements, and Regulation (EU) No 648/2012	32019R0876
Regulations	2018/1724	Establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012	32018R1724
Regulations	2017/2396	Amending Regulations (EU) No 1316/2013 and (EU) 2015/1017 as regards the extension of the duration of the European Fund for Strategic Investments as well as the introduction of the technical enhancements for that Fund and the Investment Advisory Hub	32017R2396
Regulation	2010/40/EU		

Reference to Personal Data Breach

Instrument	Reference	Name	CELEX
Directive	2016/680	on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA	32016L0680
Directive	2016/681	on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime	32016L0681
Directive	2016/1148	concerning measures for a high common level of security of network and information systems across the Union	32016L1148
Directive	2009/136/EC	amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance)	32009L0136
Regulation	2016/679	on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)	32016R0679
Regulation	2018/1725	on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.)	32018R1725
Regulation	2016/794	on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA	32016R7094
Regulation	2019/818	on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816	32019R0818
Regulation	2019/817	on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA	32019R0817
Regulation	910/2014	on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC	32014R0910
Regulation	2018/1727	on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA	32018R1727
Regulation	611/2013	on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications	32013R0611
Regulation	2017/1939	implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')	32017R1939
Regulation	2017/2226	establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011	32017R2226
Regulation	2018/1240	establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226	32018R1240
Regulation	2018/1862	on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU	32018R1862
Regulation	2018/1861	on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006	32018R1861
Regulation	526/2013	concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance	32013R0526
Regulation	2020/473	supplementing Directive (EU) 2017/2397 of the European Parliament and of the Council with regard to the standards for databases for the Union certificates of qualification, service record books and logbooks	32020R0473
Regulation	2019/1122	supplementing Directive 2003/87/EC of the European Parliament and of the Council as regards the functioning of the Union Registry (Text with EEA relevance.)	32019R1122
Regulation	2019/1715	laying down rules for the functioning of the information management system for official controls and its system components (the IMSOC Regulation) (Text with EEA relevance)	32019R1715

Congress	Reference	Name	Details
116th	H.R. 748	CARES Act	Cybersecurity Appropriations
116th	H.J. Res.31		Cybersecurity Appropriations
116th	H.R. 1158	Consolidated Appropriation Act 2020	Cybersecurity Appropriations
116th	H.R. 1865	Further Consolidated Appropriation Act 2020	Cybersecurity Appropriations
116th	H.R. 3055	Further Continuing Appropriations Act, 202 and Further Health Extenders Act of 2019	???
116th	S. 1790	National Defense Authorization Act for Fiscal Year 2020	No text available
116th	S. 1379	Pandemic and All-Hazards Preparedness and Advancing Innovation Act of 2019	Requires a report of cybersecurity threats to national health security and a strategy to prepare for, and respond to such threats.
116th	H.R. 266	Paycheck Protection Program and Health Care Enhancement Act	???
116th	S. 893	Secure 5G and Beyond	Requires a report which will contain a strategy as to how to secure the 5G network
116th	H.R. 4998	Secure and Trusted Communications Networks Act of 2019	Requires that the risk management practices will take into account the NIST cybersecurity framework
116th	H.R. 2476	Securing American Nonprofit Organizations Against Terrorism Act of 2019	Allows the use of certain funds for cybersecurity training and expenses
116th	H.R. 3151	Taxpayer First Act	Requires the IRS to plan for cybersecurity threats