This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act'
submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

Abstract

Computational Law has begun taking the role in society which has been predicted for some time. Automated decision-making and systems which assist users are now used in various jurisdictions, but with this maturity come certain caveats. Computational Law exists on the platforms which enable it, in this case digital systems, which means that it inherits the same flaws. Cybersecurity is one framework which addresses these potential weaknesses, and in this paper we go through known issues and discuss them in the various levels, from design to the physical realm. We also look at machine-learning specific adversarial problems, which entail further weaknesses. Additionally, we make certain considerations regarding computational law and existing and future legislation. Finally, we present three recommendations which are necessary for computational law to function globally, and which follow ideas in safety and security engineering. As indicated, we find that computational law must seriously consider that not only does it face the same risks as other types of software and computer systems, but that failures within it may cause financial or physical damage, as well as injustice. The consequences of Computational Legal systems failing are in this sense greater than if they were merely software and hardware. And if the system employs machine-learning, it must take note of the very specific dangers which this brings, of which data poisoning is the classic example. Computational law must also be explicitly legislated for, which we show is not the case currently in the EU, and this is also true for the cybersecurity aspects that will be relevant to it. But there is great hope in EU's proposed AI Act, which makes an important attempt at taking the specific problems which Computational Law bring into the legal sphere. Lastly, our recommendations for Computational Law and Cybersecurity are: Accommodation of threats, adequate use, and that humans must remain in the centre of their deployment. The latter is primarily for the abilities humans process and which allow them to handle emergencies.

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

The Dangers of Computational Law and Cybersecurity; Perspectives from Engineering and the AI Act

Kaspar Rosager Ludvigsen[1], Shishir Nagaraja[2], and Angela Daly[3]

[1]Department of Computer and Information Sciences, University of Strathclyde, kaspar.rosager-ludvigsen@strath.ac.uk
[2]Department of Computer and Information Sciences, University of Strathclyde, shishir.nagaraja@strath.ac.uk
[3]Leverhulme Research Centre for Forensic Science and Dundee Law School, adaly001@dundee.ac.uk

June 2022

1 Introduction

Despite law being established as an academic discipline for a significant period of time, it is still rather undefined and lacks the rigour that other disciplines possess. There are ongoing debates and unresolved questions as to when law is deductive or inductive[1], so for computational law (CL) to even claim being future-proof misses the mark. Like the existence of exotic matter in astronomy, you may deduce or assume their existence, but empirical evidence will eventually prevail and show whether it is worthwhile[2]. The same can be said for CL, as its implementation should not be forced because of powers outside the academic and legal sphere[3], or for the sake of profit. Increased use must be justified, regardless of whether some types of technology are forced upon everyone without any other reason than power[4].

CL can be defined by its usage, like many other fields of law[5]. Law in general, and CL too, contain an important modifier:

They are affected by the technological systems they exist in[6], and CL expresses this in a much more extreme manner than any other field. It would not even exist without its extra-legal roots[7]. Computer science provides the

[1]And while these are vital, we cannot discuss them further in this paper. For a contrary opinion, see footnote 4, page 98 in Ana Margarida Simões Gaudêncio, "Presumption(s) of Correctness(?): Comparing the Methodological Relevance of Precedents in Civil Law and in Common Law Systems" in *Common Law - Civil Law The Great Divide?* (Springer 2022) ⟨https://link.springer.com/chapter/10.1007/978-3-030-87718-7%7B%5C_%7D8⟩.

[2]Past questions on this are still not fully answered, see Robert A Malaney and William A Fowler, "The transformation of matter after the big bang" (1988) 76(5) American Scientist 472.

[3]Wolfgang Hoffmann-Riem, "Legal Technology/Computational Law" (2021) 1(1) Journal of Cross-disciplinary Research in Computational Law 1, 10 - 11.

[4]See any work on facial recognition or contract tracing, e.g., Isadora Neroni Rezende, "Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective" (2020) 11(3) New Journal of European Criminal Law 375; Ilia Siatitsa, "Freedom of assembly under attack: General and indiscriminate surveillance and interference with internet communications" (2020) 102(913) International Review of the Red Cross 181; Lucie White and Philippe Van Basshuysen, "Without a trace: Why did corona apps fail?" (2021) 47(12) Journal of Medical Ethics E83.

[5]See ongoing work on how this is understood, like Burkhard Schafer, *Legal Tech and Computational Legal Theory* (2022).

[6]There are diverging opinions on this, see Bert-Jaap Koops, "Should ICT Regulation Be Technology-Neutral?" in (2006) versus Paul Ohm, "The argument against technology-neutral surveillance laws" [2010] Texas Law Review.

[7]See, e.g., Louis O Kelso, "Does the Law Need a Technological Revolution?" (1946) 18 Rocky Mountain Law Review 378; W Daniel Hillis, "New computer architectures and their relationship to physics or why

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

basis and logic for CL, and in turn brings the same drawbacks[8].

A good parallel to describe this, would be the event of IoT devices[9]. The increased adoption of these brings in a new danger at every step, as all of them are (usually) connected to a network and make use of software. Every danger posed to computers and digital systems therefore exist in these devices, which are often used close to humans or for critical infrastructure, increasing the amount of possible accidents and the risk of damage[10].

CL shares this, every logical or otherwise systemic pitfall can pose a danger. For example, circumvention and adversarial law usually relies on a system that consists of courts and subjects seeking to abuse it[11]. Doing the same in CL only requires obfuscating the actions within the logic of the code or otherwise abusing technical limitations or faults of the system. The different types of parties which can do this to these systems are many times larger, than the sum of money and influence required to do this within pre-existing legal systems.

This brings us to some unique points about what kind of vulnerabilities CL will always have. Cybersecurity (which now applies to CL) consists of certain assumptions, either expressed directly or seen but not necessarily explicitly mentioned by those who practice it[12]. One of these is the assumption that there will never be a perfect defence. We are never reaching an equilibrium of defences and attacks, and the risk of incursions that can succeed will always exist. A major consequence of CL either becoming or already being implemented into national legal systems, is that they can now suffer adversarial failures (from adversarial attacks). Therefore, ironically, CL as a tool for further automation may be a target for automated adversarial attacks and loophole analysis itself.

Like in law, adversary merely refers to the subject being against the target, but the attacks and failures entail weaknesses which only increase in sophistication and consequences as the systems or technology used becomes more complicated and increasingly used. To illustrate this, imagine the difference between a court system which only partially or does not rely on CL, and one which does. The former cannot be brought to a halt or fully hijacked by an adversary. But a court system which makes fully or mostly use of CL definitely can, unless it has backups and redundancies that enables it to revert to a non-CL state.

In this sense, CL inherently makes a legal system more vulnerable, in turn potentially damaging rights, individuals, corporations and even the state itself. It is from here its relationship with cybersecurity must be scrutinised, understood and realised, which we can only discuss so much here.

In this paper, we take a very narrow look at one case, which is adversarial attacks on machine-learning (ML) models and any system that makes use of them. Computational legal systems that consist partially or fully of these, in any shape or form, will be vulnerable to attacks on the classifiers[13], one of the fundamental parts of these systems, which all the learning is used on and to form, and attacks to extract the data[14] which they are created on, or the source code of the entire system. These are all well known, but for CL, they create barriers which make the practical implementation of these systems potentially unsafe.

Safety here refers to accidents or losses, while cyberse-

computer science is no good" (1982) 21(3-4) International Journal of Theoretical Physics 255.

[8]While this is not a new or unknown phenomena, it is worth discussing and elaborating on, both to make it clearer for policymakers, users and the public in general.

[9]IoT devices can be part of a CL system, e.g., the data could feed into a system which decides on the basis of it.

[10]See any literature on this problem, Kaspar Rosager Ludvigsen and Shishir Nagaraja, "Dissecting liabilities in adversarial surgical robot failures: A national (Danish) and EU law perspective" (2022) 44 Computer Law and Security Review ⟨https://doi.org/10.1016/j.clsr.2022.105656⟩; Kevin Fu and others, "Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things" [2020] Computing Community Consortium ⟨http://arxiv.org/abs/2008.00017⟩; Syed Rizvi and others, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT" [2018] Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018 163.

[11]Extra-legal means to circumvent or abuse the legal system exist too, very much analogously to how many different ways an adversary can attack digital systems.

[12]We will not provide further argumentation for the assumptions, as these are not stringently codified in cybersecurity at the time of writing, but matter to how it is deployed in practice. For example, zero-day exploits may be dangerous, but are something you must prepare for and no one expects everything to be perfectly preventable.

[13]Matt Fredrikson, Somesh Jha, and Thomas Ristenpart, "Model inversion attacks that exploit confidence information and basic countermeasures" (2015) 2015-Octob Proceedings of the ACM Conference on Computer and Communications Security 1322.

[14]Florian Tramèr and others, "Stealing Machine Learning Models via Prediction APIs" (2016) ⟨http://arxiv.org/abs/1609.02943⟩.

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

curity refers to lowering the risk of adversarial failures. It is said that safety is increasingly covering cybersecurity[15], as seen with the IoT example above, and this implies that CL must develop defences in its technical implementation and logic. Limiting itself to ways where risks can be mitigated or hazards can be controlled is suitable, and follow the tradition of anything that absorbs cybersecurity as part of its being[16]

Section 2 defines what we see as CL and cybersecurity. After this, we discuss the weaknesses which CL contains in 5 levels. In Section 3, we dive further into machine-learning specific issues with CL, and we also comment on the problems which black boxes and authentication bring. Section 4 contains a brief legal commentary on how cybersecurity is regulated in the EU, with a focus on its effect on CL, and how the EU's future AI Act[17] may affect CL as a field. We then provide general recommendations for the future, because of the obvious consequences which CL and cybersecurity together bring in Section 5, Section 6 has some ideas for future work, and finally, Section 7 concludes the paper.

2 Computational Law and Cybersecurity

CL and cybersecurity naturally fit together, because the former interacts or exists in some digital space which requires software and/or hardware. This section combines the two and looks at weaknesses.

2.1 Definitions

CL can be defined as:

"*The techniques of computational logic, applied to the semantic rules as well as the data, form the basis of a computational law system.*[18]"

CL is considered to be automation of legal reasoning. But from the quote by Love, we can see that there are essentially two broad definitions, either purely automation or broadly applying computational logic to law. We will consider both in this paper.

2.1.1 Forms of Computational Law

To better contextualise CL, we mention selected forms here. This is not an exhaustive list, and some applications will cover several areas.

- Automated assistance within legal systems. TurboTax[19] (while not developed by a State) is always brought up, but the Danish state is another example where income and other relevant information is automatically sought and filled in[20] in tax returns and similar forms, leading to automated experiences for most subjects. On the back-end, this type of CL is also used by the authorities.

- Contract related fields, like smart contracts[21], as well as other types or derivatives, are considered CL, but are often found in their own sub genres in relation to the technology which they exist in. These see primarily use in private law[22], and will not always be able to execute their contents fully without assistance from litigation or other means[23]. The latter comes

[15] Acknowledged by the European Union, see page 10 of 'MDCG 2019-16 Guidance on Cybersecurity for medical devices', ⟨https://ec.europa.eu/docsroom/documents/41863⟩, last accessed 30 June 2022.

[16] Ibid. But any type of product which gains network connectivity could be a good example. For a general overview in the EU, see Cezary Banasiński and Marcin Rojszczak, "Cybersecurity of consumer products against the background of the EU model of cyberspace protection" (2021) 7(1) Journal of Cybersecurity 1.

[17] Proposal for a Regulation of the European Parliament and of the Council laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206.

[18] Nathaniel Love and Michael Genesereth, "Computational Law" [2005] ICAIL 205, 206.

[19] See Kacey Marr, "You're Only as Good as Your Tax Software: The Tax Court's Wrongful Approval of the Turbotax Defense in Olsen v. Commissioner" (2012) 81(2) University of Cincinnati Law Review 709, for an example of function and issues.

[20] https://lifeindenmark.borger.dk/economy-and-tax/the-danish-tax-system/a-general-introduction-to-the-danish-tax-system, last accessed 30 June 2022.

[21] Abhishek Dixit and others, "Towards user-centered and legally relevant smart-contract development: A systematic literature review" (2022) 26(November 2021) Journal of Industrial Information Integration 100314 ⟨https://doi.org/10.1016/j.jii.2021.100314⟩.

[22] However, even public authorities and states will be private law subjects to the companies they create contractual relations with.

[23] For an elaboration of these issues, see Pablo Sanz Bayón, "Key Legal Issues Surrounding Smart Contract Applications" (2019) 1 KLRI; Monika Di Angelo, Alfred Soare, and Gernot Salzer, "Smart contracts

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

down to needing state or legal system assistance to fulfill them, in case of disputes or disagreements.

- Automated legal decision-making. This can range from public legal decisions on subsidies, pension, automated payments[24] or company registration, with a much bigger potential in the future[25]. For future applications, the research community and the industry as such tends to focus on automated tools or AI judges[26] but this seems very far-fetched with the capabilities of current CL systems.

- Quantum CL, if the event of quantum computing occurs, should be its own separate field[27]. Primarily due to the power imbalance, but also the new physical constraints of the system. The former refers to the substantially increased amount of computing power these will have over conventional hardware, the latter to the real tangible physical difference which quantum computers contain, meaning that new threat models and measures will have to be developed[28].

What these all have in common, is that they exist in or as software and make use of hardware, while containing a level of automation and operate within or as the legal system. This entails that cybersecurity is an issue for all of them.

2.1.2 Cybersecurity

Cybersecurity can be defined as freedom from adversarial failures[29], but there exists other definitions outside of traditional security engineering. We chose this because it is narrow and focused on mitigating or limiting the damage of what failure to defend against attacks may cause.

As mentioned, this freedom is hard to attain, and it is therefore more of a goal to strive for, than a goal to reach[30]. Adversaries successfully attacking a system does not always lead to safety failures, but with the few examples we have mentioned, there is a risk they will. Safety is the general idea of freedom from accidents or losses[31], where both financial as well as human losses are included.

Cybersecurity itself is very diverse, and includes everything from encryption, good practice for building databases[32] and naming conventions[33], to physical elements like air gaps[34], or access control[35] to both the servers or robots[36].

What we focus on is the additional layer of complexity and potential risk which cybersecurity adds to CL. Very much like safety engineering with the event of the industrial revolution, cybersecurity needs to be integrated and

in view of the civil code" (2019) Part F1477 Proceedings of the ACM Symposium on Applied Computing 392; Kevin Werbach and Nicolas Cornell, "Contracts Ex Ma China" (2017) 67(2) Duke Law Journal.

[24] The wrongful texts on Estonian AI should have referred to the development of automated systems for certain types of payment, see https://www.just.ee/en/news/estonia-does-not-develop-ai-judge, last accessed 30 June 2022.

[25] For an overview in public legal systems, see Ulrik BU Roehl, "Understanding Automated Decision-Making in the Public Sector: A Classification of Automated, Administrative Decision-Making" in *Service Automation in the Public Sector* (Springer 2022) ⟨https://link.springer.com/10.1007/978-3-030-92644-1%7B%5C_%7D3⟩.

[26] Some examples could be John Morison and Adam Harkens, "Re-engineering justice? Robot judges, computerised courts and (semi) automated legal decision-making" (2019) 39(4) Legal Studies 618; Nu Wang, ""Black Box Justice": Robot Judges and AI-based Judgement Processes in China's Court System" [2020] International Symposium on Technology and Society 58; Fabrice Muhlenbach, Long Nguyen Phuoc, and Isabelle Sayn, "Predicting Court Decisions for Alimony: Avoiding Extra-legal Factors in Decision made by Judges and Not Understandable AI Models" (2020) ⟨http://arxiv.org/abs/2007.04824⟩.

[27] Jeffery Atik and Valentin Jeutner, "Quantum computing and computational law" (2021) 13(2) Law, Innovation and Technology 302 ⟨https://doi.org/10.1080/17579961.2021.1977216⟩, 305.

[28] There is a wealth of post-quantum research which is ongoing, see, e.g., Jongmin Ahn and others, "Toward Quantum Secured Distributed Energy Resources: Adoption of Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD)" (2022) 15(3) Energies.

[29] Nancy G Leveson, *Safeware: System Safety and Computers* (1., Addison-Wesley Publishing Company, Inc 1995).

[30] And can be expanded to include the process of attaining security, see Tomasz Zdzikot, "Cyberspace and Cybersecurity" in *Cybersecurity in Poland* (2022) 17 - 18.

[31] Leveson (n 29).

[32] Habib Ibrahim, Songul Karabatak, and Abdullahi Abba Abdullahi, "A Study on Cybersecurity Challenges in E-learning and Database Management System" [2020] 8th International Symposium on Digital Forensics and Security, ISDFS 2020.

[33] Ross Anderson, *Security engineering: a guide to building dependable distributed systems* (John Wiley & Sons 2020) 259-271.

[34] Physical gaps between the system and the internet or just public space. Guri has written a range of papers on how to mitigate and understand air gaps, see e.g., Mordechai Guri, "Lantenna: Exfiltrating data from air-gapped networks via ethernet cables emission" [2021] Proceedings - 2021 IEEE 45th Annual Computers, Software, and Applications Conference, COMPSAC 2021 745.

[35] Adriano Valenzano, "Industrial cybersecurity: Improving security through access control policy models" (2014) 8(2) IEEE Industrial Electronics Magazine 6.

[36] Each area could be analysed specifically with regards to CL, but this is not the paper for that.

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

considered when designing and also deploying CL systems. Gone are the days where the application and idea behind CL is purely discussed, as there are weaknesses which certain types of logic or choices add, giving rise to practical impacts.

2.2 Weaknesses

CL can exist in a theoretical manner without considering cybersecurity, but when deployed in practice, defences are needed in various ways. Stochastic or completely unpredictable issues are not considered because of their extraordinary nature. But the limitations to what can be considered special enough to warrant lack of liability depends on the jurisdiction, to this, see our past work[37], for an analysis combining private law and cybersecurity within a Danish context.

2.2.1 General Issues

With inspiration from existing literature, we sketch an overarching conceptual understanding of how cybersecurity matters to CL.

Weakness in CL can be described in the following levels:

1. Logic or design.
2. Software.
3. Hardware.
4. System or network.
5. Physical.

If the logic or the design of the system does not consider most common threats, and has not been thoroughly tested, cybersecurity adds a layer of weakness to all levels. Testing for hardware is the same as software, but level 4 is different.

Broadly, all the attacks and defences work on individual levels (each substation), but if these are not applied uniformly, the weakness will consist of other systems (not those related to the CL), because individual weaknesses will impose a risk on everyone in the system, making level 4 exceptionally difficult. This includes the very network(s) that CL use.

Atttacks on the physical layer, level 5, is to usually enable an attack on a lower level, except for those unique to it such as physical destruction, but shoulder-surfing[38] or physical side-channel attacks[39] are examples of the first.

Most levels are described or specified better in existing literature. Regardless of this, there are some unique additional explanations needed for each.

To illustrate the division, we include an visualisation which shows the interactions between the different levels.

2.2.2 Logic

Cybersecurity confer devastating and potentially permanent weaknesses to CL systems through its choice of logic, as it is what defines what should be understood and done. This is explained by how it is constructed, e.g., through the use of machine-learning or expert decision-making, or through choices of programming language or other technical design decisions. These must be not only uncovered and possibly mitigated, but some may warrant the removal of the system entirely, if any of the core weaknesses compromise any basic cybersecurity attributes at large. For example, machine-learning based systems may contain weaknesses that allow both data and the code behind it to be easily retrievable, and if defences against this are not vigilantly updated and improved throughout the life-cycle of the system, they should not even be used in the first place.

Another could be the logic behind what constitutes a decision in the system[40], becoming law, which may be circumventable or possible to be hijacked, either through

[37] Ludvigsen and Nagaraja, "Dissecting liabilities in adversarial surgical robot failures: A national (Danish) and EU law perspective" (n 10).

[38] Refers to snooping, observing literally over a shoulder or otherwise, to deduce or directly observe passwords or other information. There exists plenty of research on the matter, see, e.g., Mihai Bâce and others, "PrivacyScout : Assessing Vulnerability to Shoulder Surfing on Mobile Devices" (2022) 21(1) Proceedings on Privacy Enhancing Technologies 1.

[39] Physical, unlike digital side-channel attacks, refers to readings which then allow an adversary to manipulate or otherwise know something they should not. This could be electromagnetic and so on, see following article for a great overview with a focus on neural networks, Maria Méndez Real and Rubén Salvador, "Physical side-channel attacks on embedded neural networks: A survey" (2021) 11(15) Applied Sciences (Switzerland).

[40] This applies to all types of platforms CL can use.

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

known techniques or some discovered by fuzzing[41]. Circumvention or hijacking can be seen as obfuscation or abuse by known constraints of the system, which is known in law as:

Loopholes[42], deliberate non-compliance without enforcement[43] or stalling for time[44] through litigation or in public law[45]. CL allows circumvention etc., that does not necessarily require humans or much effort measured by time, which increases the risk as to whether it will be used[46].

2.2.3 Software

CL is expressed in and usually executes within the software level. Pandora's box is therefore opened in regards to weaknesses, anything that is possible with the very software[47] that is or the CL resides in, expresses the opportunities of attack and failures. This could be in the form of denial-of-service of various kinds, leading to loss of integrity or availability. The latter is especially important if the CL is the only source of decisions on for example legal subsidies or permits, and if such a system is taken out, and there are no redundancies, systemic financial loss is very possible[48]. Software is usually also the target of attacks from the other levels, and attacking the CL software is very possible through other software in the system somewhere, which we focus on further below.

2.2.4 Hardware

Attacking software through hardware is classic, as seen with the Spectre attack on CPUs[49], and recently Hertzbleed[50], allow for various actions going from hardware to software. In a CL context, this would allow attackers everything from stealing data, to escalation attacks that would give them control of the software, or simply a way to destroy it through ransomware attacks with no way to reverse the encryption of files.

Defences against this are often physical, but as attacks like Spook.js[51] show, you do not even need to have such access to perform the attack. In this sense, hardware only adds to the burden of defending CL systems, and the most important detail of all here, is there is no way to prevent all side or covert channels from being exploited, as they often are caused by deliberate decisions in hardware architecture. This is best seen with the Spectre attack and its derivatives, as the weakness that allows it also increases CPU performance immensely, and will therefore not (unless by law) be changed or removed. Analogies to this will exist in many types of hardware.

2.2.5 System

As mentioned above, attacks from other types of software towards the one which the CL system resides in is

[41] Fuzzing is the practice of testing arbitrary or deliberate inputs or actions, and seeing how the system reacts to it. Some that can cause adversarial attacks may be discovered at the design stage, others later. For an overview, see Richard Mcnally, Ken Yiu, and Duncan Grove, *Fuzzing : The State of the Art* (techspace rep, DSTO Defence Science and Technology Organisation 2012).

[42] There exists an ocean of research on the concept, good specialised examples could be Matthew R Espinosa, "Small Business Cybersecurity: A Loophole to Consumer Data" (2022) 24(2) The Scolar: St. Mary's Law Review on Race and Social Justice; Grant Butler, "The Sky Reefer Loophole : How Modern Carriers Lessen Their Liability Through Foreign Arbitration and Choice of Court Provisions-and Four Countries Who Stopped It" (2022) 46(1) Tulane Maritime Law Journal.

[43] For an empirical study with interesting perspectives on this, see Aliu Oladimeji Shodunke, "Enforcement of COVID-19 pandemic lockdown orders in Nigeria: Evidence of public (Non)compliance and police illegalities" (2022) 77(May) International Journal of Disaster Risk Reduction 103082 ⟨https://doi.org/10.1016/j.ijdrr.2022.103082⟩.

[44] Joanna Mazur and Marcin Serafin, "Stalling the State: How Digital Platforms Contribute to and Profit From Delays in the Enforcement and Adoption of Regulations" [2022] Comparative Political Studies 001041402210896 ⟨http://journals.sagepub.com/doi/10.1177/00104140221089651⟩.

[45] This list in not exhaustive, but represents common areas.

[46] Cheap externalities usually leads to increased use, as we have seen with the data sharing, see, e.g., Shota Ichihashi, "The economics of data externalities" (2021) 196 Journal of Economic Theory 105316 ⟨https://doi.org/10.1016/j.jet.2021.105316⟩. Worth noting that even if elements make higher profits for shareholders, this does not mean decreased costs for users or better rights, see Ronald J Deibert, "Subversion Inc: The Age of Private Espionage" (2022) 33(2) Journal of Democracy 28. This analogy persists with CL as well, as it will end up being extremely cheap to attack and abuse the systems going forward.

[47] This could be the AI that decides, or one of several subsystems.

[48] As is mental damage to those who are denied finances to live from, as could be the case with pension or other types of social services.

[49] There exist many good papers on defences and solutions against it, see e.g., Mohd Fadzil Abdul Kadir and others, "Retpoline technique for mitigating spectre attack" [2019] Proceedings - 2019 6th International Conference on Electrical and Electronics Engineering, ICEEE 2019 96.

[50] Yingchen Wang and others, "Hertzbleed : Turning Power Side-Channel Attacks Into Remote Timing Attacks on x86" (2022).

[51] Ayush Agarwal and others, "Spook.js: Attacking Chrome Strict Site Isolation via Speculative Execution" [2022] .

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

the biggest threat overall. Spook.js[52] does this partially too, as it enables attacks in the browser, which in a CL context could result in an adversary stealing information from singular users accessing CL decisions or data which is being provided to such a a system. On the provider end, operation systems, proprietary software or even malicious antivirus[53] or just plain malware, can all cause one or several types of software or potentially hardware to be compromised. In this context, the weakness is the entire infrastructure where we rely on many types of software and hardware at once.

Solutions like trusted or trustworthy[54] hardware are not enough, and attackers merely need to exploit or use well known techniques to gain some type of access, then lie in wait until they can use their position to potentially reach the system which houses the CL. Even from the perspective of the user, weaknesses on their side may allow adversaries to manipulate or violate the confidentiality of CL system, adding an additional attack venue. In this sense, the system level weakness of CL is most likely the most severe, as the potential battlefield of different options and tools which adversaries can use are frankly many times greater than any of the others.

2.2.6 Physical

Destroying servers physically, or abusing physical interfaces such as USB[55] all constitute primary reasons to have backups and redundancies for CL systems. Physical attacks, unless aimed at destruction, will be means to escalate and gain access to hardware and software. It may seem like the simplest area, but defending and perhaps expecting employees to abuse their knowledge of location of servers and so on, is in its own way paramount in cybersecurity regarding CL systems.

As mentioned, physical side-channel attacks are another matter where defences must be erected, but many types will regrettably always exist due to their passive or irreplaceable nature[56], either due to the costs for preventing any leakage or disabling designs which are necessary for the functioning of the hardware.

2.3 Strengths

On the contrary, CL does contain certain strengths over non-computational systems. Distributed and massive decision-making[57], simplified and efficient support and search powers (to help users or citizens) and the other classic benefits of automation apply[58]. However, all of it requires the right kind of humans in-the-loop and legislative framework. Assuming the latter is true in a system, the strengths of CL are quite clear. Regardless of this, the strengths may not outweigh the costs, which we will comment on later.

3 Cases

To specifically illustrate the interaction between CL and cybersecurity, we take a look at some examples.

3.1 Machine-Learning Specific Issues

Existing taxonomies and threat models for machine-learning (ML) models and systems sufficiently describe the problem [59]. But in the context of CL, we can deliber-

[52] Agarwal and others (n 51).

[53] Gopalakrishnan Prakash and Marimuthu Parameswari, "On reviewing the implications of Rogue Antivirus" (2016) 25(2) Journal of Information Ethics 128.

[54] Trustworthy must be made to never fail, whereas trusted merely is the idea that it should not fail, but there is no assurance it never will, Anderson (n 33) 13.

[55] Tyler Thomas and others, "Duck Hunt: Memory forensics of USB attack platforms" (2021) 37 Forensic Science International: Digital Investigation 301190 ⟨https://doi.org/10.1016/j.fsidi.2021.301190⟩.

[56] Electromagnetic emissions are close to impossible to prevent efficiently in all systems, which means this can usually always be deployed. For insights into this, see Asanka P Sayakkara and Nhien An Le-Khac, "Forensic insights from smartphones through electromagnetic side-channel analysis" (2021) 9 IEEE Access 13237; Asanka Sayakkara, Nhien An Le-Khac, and Mark Scanlon, "A survey of electromagnetic side-channel attacks and discussion on their case-progressing potential for digital forensics" (2019) 29 Digital Investigation 43 ⟨https://doi.org/10.1016/j.diin.2019.03.002⟩. It could also be audio, anything that can reveal the inner workings of hardware is possible to make use of.

[57] On the contrary, see Jennifer Cobbe, "Administrative law and the machines of government: Judicial review of automated public-sector decision-making" (2019) 39(4) Legal Studies 636.

[58] While this is contentious, and requires more empirical research to confirm, there are indications towards this direction, see Monika Zalnieriute, Lyria Bennett Moses, and George Williams, "The rule of law and automation of government decision-making" (2019) 82(3) Modern Law Review 425.

[59] See examples like Rajesh Gupta and others, "Machine Learning Models for Secure Data Analytics: A taxonomy and threat model"

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

ately go past the CIA triad, confidentiality, integrity and availability[60], and focus on:

1. Poisoning (modification) or possession of the training data.
2. Attacks on the model or during the creation of it.
3. Hijacking of the communication from or to the model or where it operates.

3.1.1 Poisoning or possession of data

For ML based CL systems, this is where the biggest risk lies. Not only can all training data, personal or not, be stolen and published or used to make a competitive model, but these can also result in consequences which cannot be seen until the system has made an unfair or outright dangerous decision. Even if it did not matter whether the SyRi system was ML based or not[61], an attack with similar or more severe consequences like in the Post Office case[62], could be caused by deliberately changing the data to make a system commit to wrong decisions or actions. There are defences, but vigilance by every human involved, combined with an understanding that data may be poisoned in the first place, and regular auditing, must be prioritised to minimize the threat which this constitutes.

3.1.2 Model Attacks

Not unlike other types of software, protecting the model at the design stage is vital, as adversaries can inject or modify parts which may, like above, cause decisions with very legal or physical consequences due to its CL nature[63]. Unlike poisoning, model attacks may be used by journalists and competitors to attempt to reveal the contents of the model for various purposes. Activism in cybersecurity is well known[64], and may play a role here and elsewhere, and with the position CL takes in society, this clash may be further exacerbated. Like other types of activism, which include activities that may be considered criminal, this is typically divided into black[65], white[66] and grey hatted[67], but what matters the most, is the danger that each possess. This must be considered before using CL with ML, as the adversaries may cause undesirable outcomes for the provider, user and citizen respectively, explicitly by revealing the model illegally, ethically or unethically.

3.1.3 Communication Attacks

While less dangerous than the two others, and seen heavily elsewhere in various ways, communication attacks, if done in a CL system with multiple steps, could potentially cause some of the same issues as above. Traditionally, these are divided into several categories, such as replay, hijacking or modification. The central part is that what is sent and received is attacked, not necessarily the software itself, in this sense its actions[68]. Contents of the commu-

(2020) 153(February) Computer Communications 406 ⟨https://doi.org/10.1016/j.comcom.2020.02.008⟩; Nicolas Papernot and others, "SoK: Security and Privacy in Machine Learning" [2018] Proceedings - 3rd IEEE European Symposium on Security and Privacy, EURO S and P 2018 399. For a practical summary of the current threat model landscape, see https://docs.microsoft.com/en-us/security/engineering/threat-modeling-aiml, last accessed 30 June 2022.

[60] Failures in each may overlap during specific successful attacks. The CIA triad is a core concept in cybersecurity at large, and is understood in a literal sense.

[61] Adamantia Rachovitsa and Niclas Johann, "The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case" (2022) 22(2) Human Rights Law Review 1.

[62] James Christie, "The post office horizon it scandal and the presumption of the dependability of computer evidence" (2020) 17(March) Digital Evidence and Electronic Signature Law Review 49. The loss of lives were a later consequence, but are still significant.

[63] Or simply steal the model and use it for themselves.

[64] There exists plenty of research on this, from many different types of sciences, e.g., Jordana George and Dorothy E Leidner, "Digital activism: A hierarchy of political commitment" (2018) 2018-Janua Proceedings of the Annual Hawaii International Conference on System Sciences 2299.

[65] KHazel Kwon and Jana Shakarian, "Black-Hat Hackers' Crisis Information Processing in the Darknet: A Case Study of Cyber Underground Market Shutdowns" in *In Networks, Hacking, and Media – CITA MS@30: Now and Then and Tomorrow.* (November 2018) ⟨https://www.emerald.com/insight/content/doi/10.1108/S2050-206020180000017007/full/html⟩.

[66] Andrew R Schrock, "Civic hacking as data activism and advocacy: A history from publicity to open government data" (2016) 18(4) New Media and Society 581.

[67] Georg Thomas, Oliver Burmeister, and Gregory Low, "The Importance of Ethical Conduct by Penetration Testers in the Age of Breach Disclosure Laws." (2019) 23 Australasian Journal of Information Systems 1.

[68] Papers which give an overview on this are, e.g., Paul Syverson, "A Taxonomy of Replay Attacks" [1994] Proceedings The Computer Security Foundations Workshop VII 187 ⟨http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=315935⟩; Christos Xenofontos and others, "Consumer, Commercial, and Industrial IoT (In)Security: Attack Taxonomy and Case Studies" (2022) 9(1) IEEE Internet of Things Journal 199; Peter Huitsing and others, "Attack taxonomies for the Modbus

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

nication could lead to changes in decisions, or the system could just stop functioning from wrong received input.

3.2 Black Boxes

Black boxes may exist deliberately, or for political or unknown reasons, but from a cybersecurity perspective, they are not wanted or useful. Trade-secrets or patents can warrant this, but the general idea is strong security, not secrecy[69]. CL suffers further from this through the loss of legitimacy. Transparency and openness about what a system can and should do will increase trust and confidence and vice versa. The exceptions for this would be surveillance or military purposes, but even these should still be as strong as possible[70]. ML based solutions may be Black Boxes for the two reasons mentioned above, but another could be the complexity of the neural network which supports it. The question then becomes whether CL systems should make use of such technology, if it is not possible to comprehend or in a transparent manner show what goes on inside of it. Considering the weight which CL systems in the future may have, in both a human and legal manner, it may simply not be advisable to use them on this basis alone. Outside the reasoning above, it could also be due to the security worries which a system you do not know or understand can have.

3.3 Authentication

When authentication[71] is automated in a digital manner, it will be considered as being part of CL, regardless of whether it is incorporated or interpreted into the legal system.

But, authentication has a known amount of problems, such as proliferation of new technology, which does not solve its issues[72], its practical constraints through circumvention[73] or coercion, and lack of empirical research that really considers the population at large and not just students or paid individuals as the data source.

CL in authentication refers to the legal identification of the individual, either through a legal decision or as part of a process, and includes access to the state, banks and other companies which may constitute critical or important digital infrastructure in the lives of individuals. The conflict occurs when the CL is faulty, either deliberately or not, and leads to injustice or financial losses. Not unlike law in general, there is no quick solution, and CL must guarantee humans-in-the-loop to function in practice.

In terms of cybersecurity, authentication may be an enabler for fraud through impersonation or integrity loss. Unlike past means of fraud, authentication in CL enables these actions to be done remotely and at a massive scale, which lowers the financial and practical costs and increases the risk of occurrence dramatically. This must be countered on a design or software level, but is rarely the focus of developers and users of these systems.

4 Cybersecurity Legislation

While there is little concrete and hard law which directly regulates cybersecurity[74], we do have certain EU legislation which specifies elements of it.

4.1 The Cybersecurity Regulation and Future Legislation

Currently, cybersecurity in the EU is regulated on a product to product type basis via guidance[75], somewhat dedi-

protocols" (2008) 1(C) International Journal of Critical Infrastructure Protection 37 ⟨http://dx.doi.org/10.1016/j.ijcip.2008.08.003⟩.

[69] Auguste Kerckhoffs, "La cryptographie militaire" (1883) IX Journal des sciences militaires 5 ⟨http : / / www . petitcolas . net / fabien / kerckhoffs/⟩.

[70] ibid.

[71] For good taxonomy based overviews, see Mohammed El-Hajj and others, "Analysis of authentication techniques in Internet of Things (IoT)" (2017) 2017-Janua 2017 1st Cyber Security in Networking Conference, CSNet 2017 1; Sravani Challa and others, "Authentication Protocols for Implantable Medical Devices: Taxonomy, Analysis and Future Directions" (2018) 7(1) IEEE Consumer Electronics Magazine 57.

[72] Sander Joos and others, *Adversarial Robustness is Not Enough: Practical Limitations for Securing Facial Authentication* (1, vol 1, Association for Computing Machinery 2022).

[73] Jim Blythe, Ross Koppel, and Sean W Smith, "Circumvention of security: Good users do bad things" (2013) 11(5) IEEE Security and Privacy 80.

[74] This statement can be contested, on the basis that many jurisdictions will have overarching rules and legislation which may sound like it regulates it. The problem with a majority of these is that they leave the technical questions to guidance or worse, standards, without enforcement by professionals who actually understand these attributes. A further comparative legal analysis of this should be done elsewhere.

[75] If medical devices are used as an example, see our commentary on the role which cybersecurity guidance has in: Ludvigsen and Na-

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

cated rules[76], through the NIS directive[77] in a national and fragmented manner, strictly by the Cybersecurity Act[78] which only applies to EU institutions, and coordinated in a semi-volunteered manner by ENISA via the Cybersecurity Act. On the sidelines, we do have standards and other measures that may be enforced on a contractual or national basis, but they come with the usual caveats. For CL, this means that until there is harder law specifying which techniques should and should not be used, it will exist in a grey area. Yet again, CL will be treated like other types of software and systems, even if there should perhaps be specialised rules to accommodate the increased risks caused by failure, not unlike the cybersecurity requirements that exist for critical infrastructure like telecommunication[79].

4.1.1 Cybersecurity Resilience Act

Earlier in 2022, the Commission called for evidence for a future Cybersecurity Resilience Act[80]. We provided commentary for this, but there are some further considerations when discussing CL. Resilience is usually defined as a system that enables detection, tolerance and recovery from issues[81]. The problem with CL, is that there must be adequate legislation and redundancies and mechanisms, not just technical or engineering based solutions. Real resilience in CL is thus only attained when we have had to time study the failures and issues of past systems, such as the SyRi case[82], and this is traditionally how we improve both safety and security. Resilience in CL must therefore be a matter of increased redundancy, in the form of subsidiary systems or humans which can take over roles of the CL system in an emergency, strict logic and design which focuses heavily on preventing adversarial or non-adversarial failures through standards or existing research on issues and problems with the hardware or software used, and recovery mechanisms which allow the CL system to keep functioning either partially or fully after disruption of any kind. The latter should be both recovery from actions of the system, so that the resources (time, financial) are not wasted, but also in a classic sense, where it can recover from attacks which bring down the or partially hijacks the system. There is currently no interest in creating these in the future Cybersecurity Resilience Act, but there may be another approach to this problem.

4.2 Artificial Intelligence Act

CL will become part of the European product legislation world via the proposed AI Act[83]. This means that both its cybersecurity[84] and its mechanisms as artificial intelligence[85] will be the subject of regulation. How much and and of which kind remains to be seen, as the Act has not been finalised yet. Irrespective of the progress of the Act, we can draw some general considerations which CL bring. The proposed AI Act allows the EU to regulate CL

garaja, "Dissecting liabilities in adversarial surgical robot failures: A national (Danish) and EU law perspective" (n 10); Kaspar Ludvigsen, Shishir Nagaraja, and Angela Daly, "When Is Software a Medical Device? Understanding and Determining the "Intention" and Requirements for Software as a Medical Device in European Union Law" [2021] European Journal of Risk Regulation 1. For other perspectives, see Banasiński and Rojszczak (n 16); Pier Giorgio Chiara, "The IoT and the new EU cybersecurity regulatory landscape" [2022] (May) International Review of Law, Computers and Technology 1 ⟨https://doi.org/10.1080/13600869.2022.2060468⟩.

[76] Each type has its own Regulations and Directives. For a good example, see Regulation 2019/941 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC regarding critical infrastructure, [2019], L 158/1. Note that this is still not centralised hard law, but delegation. For general commentary, see Leandros A Maglaras and others, "Cyber security of critical infrastructures" (2018) 4(1) ICT Express 42 ⟨https://doi.org/10.1016/j.icte.2018.02.001⟩.

[77] Directive 2016/1148, concerning measures for a high common level of security of network and information systems across the Union, [2016] L 194/1.

[78] Through Regulation 2019/81 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU)No 526/2013 (Cybersecurity Act), [2019] L 151/15.

[79] See Edyta Karolina Szczepaniuk and Hubert Szczepaniuk, "Analysis of cybersecurity competencies: Recommendations for telecommunications policy" (2022) 46(3) Telecommunications Policy 102282 ⟨https://doi.org/10.1016/j.telpol.2021.102282⟩ for analysis on human factors in it.

[80] See Kaspar Rosager Ludvigsen and Shishir Nagaraja, "The Opportunity to Regulate Cybersecurity in the EU (and the World): Recommendations for the Cybersecurity Resilience Act" [2022] 1 ⟨http://arxiv.org/abs/2205.13196⟩.

[81] Defined more narrowly and precisely in Anderson (n 33) 251 - 252.

[82] Rachovitsa and Johann (n 61).

[83] Proposal for a Regulation of the European Parliament and of the Council laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206.

[84] Art 15.

[85] Through what kind of risk it constitutes, which a lot of the time will be high, see Art 6(2) and Annex III. CL can fit many of the categories specified in Annex III, which means it will mostly be considered High Risk AI.

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

in a practical manner, and since the type depends on the area which the CL system functions in, it can either draw rules from there[86], or perhaps be granted new guidance which it must follow under the supervision of National Competent Authorities (authorities). Sadly, if the same type of loose enforcement seen in other types of product legislation continues, there is a risk of easy circumvention or mere loose slaps on the wrists for private or public providers of CL, which may not be very beneficial for the subjects which will be affected by poorly secured CL systems.

4.2.1 Cybersecurity and Resilience

Let us *firstly* take a closer look at Article 15:

"*1. High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle. ...*"

The AI Act considers robustness and cybersecurity here, and the wording is much clearer and closer to the expectations of those that build these systems. The Article continues with:

"*... 3. High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans. High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations ('feedback loops') are duly addressed with appropriate mitigation measures. ...*"

As CL will mostly be considered High-risk, these rules will apply directly. The definition of resilience here excludes what is considered robustness, but in a combined understanding, the Article covers what resilience traditionally is. All in all, these are clear and well aligned with best practice, and even include considerations which we did earlier regarding machine-learning. The main problem then becomes enforcement, and whether those that use or develop the systems will actually adhere to the rules.

4.2.2 Human Oversight

Secondarily, the AI Act also considers human oversight in Article 14, which from a literal reading does come very close to the kind of rules needed to regulate CL adequately:

"*1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.*"

"*2. Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in this Chapter. ...*"

Article 14(1) and 14(2) entail effective oversight, a rather strong and non-negotiable position, which warrants transparency and ease of use, perhaps an issue for CL systems which make use of machine-learning. Minimizing risk via human oversight is very sound, especially regarding misuse[87]. Continuing this, Article 14(3) requires built and implemented or identified human oversight by the provider. This is a logical extension of the ideas above. Article 14(4) specifies exactly what the human oversight should be capable off, effectively professional or system requirements, including full understanding, tendency and bias awareness, correct interpretation, knowing when to disregard the AI, and being able to intervene or stop the system.

Overall, Article 14 has taken all of the best elements of how humans in-the-loop should be implemented, and expressed it in a fairly comprehensive manner. Regarding CL, the complexity will exist in how the system handles and understands the law, and the Article does not resolve this issue, but definitely leads the way. However, like above, we are left without opportunities for sanction-

[86] Various product legislation will work alongside the AI Act, see Art 6(2) and Annex II.

[87] Which could be adversarial failures.

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

ing, and there are no concrete definitions to find here or in the Annexes as to what exact behaviour we are looking for, as this will be fairly complicated when actually defined narrowly in internal rules or guidance. This is unlike cybersecurity, where techniques and concepts like requiring encryption and air gaps are fairly technical, but very possible to require in hard law.

4.2.3 Enforcement

The enforcement structure is quite important to consider when discussing CL, as there will be a certain overlap between it and AI. Ideally, the AI Act ends up in a form or is accompanied by additional regulation which enables it to handle the specific consequences of CL as AI rather well[88], but in its current form, this is not the case. However, the AI Act is equipped with obligations and requirements, and some means to enforce them, albeit not as harshly or directly as many had wanted[89]. The obligations are found in Articles 16 - 24 and 61 - 62, specifically for providers[90]. There are additional enforcement measures in Articles 63 - 68, which may partially rely on the obligations above. Like other product legislation, the authority is (usually) not the body which will technically test whether the product conforms with the rules. Instead, this is done by Notified Bodies[91], which will likely be private organisations, again a parallel to existing systems in, e.g., the medical device world in the EU. Secondarily, you have the aforementioned National Competent Authorities[92] who also act as Notifying Authorities[93]. Most of the duty of care or fulfillment of responsibilities, and even reporting, are put on the shoulders of the providers. In a CL context, this can be rather dangerous, as the 15 day notice in Article 62, by virtue of how long it is, can cause massive damage to individuals wrongfully decided on or assisted by the CL system. The enforcement mechanisms themselves rely on Article 64, which should give the authorities access to pretty much everything regarding the AI, but for them to independently step in and investigate, there must be a risk at a national level[94]. CL will not fulfill the requirements to be considered a risk on this stage, so Article 67 or 68 must be used instead. Using the same evaluation as in Article 65, the authority can force the provider of AI to withdraw and, if possible, repair and prevent the risk which the AI poses[95]. Worth noting is the definition of risk or breach of obligations in Article 67(1):

"*... it presents a risk to the health or safety of persons, to the compliance with obligations under Union or national law intended to protect fundamental rights or to other aspects of public interest protection ...*"

For CL, the latter part is intrinsically relevant, and if literally and loyally followed, could be the supporting stone which CL needs in its proper deployment. The problem then becomes the authorities themselves, *whether they will realise and act on this in time* and other general enforcement issues. The first is (uniquely) answered in Article 59(4), but this can be abused or deliberately not followed, causing the authority to become inactive or at least barely functioning. For the second part, the wording in Article 65(2) is ambiguous, and can be interpreted in a variety of ways. If we follow the logic and ideas from existing product legislation[96], it must rely on self-reporting[97] or information from other national authorities, or worse, through disclosures from journalists or researchers in an informal manner. Lastly, the AI Act delegates the means which the authorities can withdraw or otherwise sanction the providers to the Member States, which sadly gives little certainty going forward. In a CL context, this means that ongoing injustice or financial damage could take a long time be discovered and resolved, and in this sense, an *ex ante* review mechanism of the AI with CL features would be much more adequate.

[88] If Annex I stays in its current shape, all CL will be considered AI unless they provide assistance, but even some of these may pass.

[89] See critical analysis in Vera Lúcia Raposo, "Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence" (2022) 30(1) International Journal of Law and Information Technology 88 for more.

[90] Additional obligations for importers and distributors exist as well, and uniquely, some obligations for users, which is extremely important for CL systems. This is because unintended use or unexpected consequences, in litigation, may hinge on who caused it or additionally, product liability rules.

[91] Art 33, but be aware of the role which subsidiaries will play, see Art 34 for this.

[92] Art 59.

[93] Art 30.

[94] Art 65(2).

[95] Art 67(1).

[96] And since there is nothing explicitly stating when, where, and how market surveillance could ideally be done on AI in the AI Act.

[97] Art 61 and 62.

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

5 Recommendations

If we consider the clash that CL and cybersecurity bring, we can combine it with common sense arguments from both safety and security engineering, and the ideas found in the AI Act, forming three recommendations:

1. CL systems must accommodate the cybersecurity threats which they can include, at a design, deployment and post-deployment level (life-cycle), considering all levels of weakness.
2. CL systems should only be used when adequate, as it is not a silver bullet for every problem it is applied to. Adequate analysis and predictions must be independently made, with the caveats which this brings through likelihood and assumptions.
3. Humans must still play a role in CL, as they represent plasticity, adaptability and arbitration, values which no CL system can possess. This is the only way which the systems can handle unexpected occurrences, systemic injustice and other difficulties.

5.1 Comments

While these are more general and will apply to a general comprehension of CL and cybersecurity in general, details and the understanding of each must be commented on briefly.

First recommendation. This concerns itself with defences and mitigation measures towards adversarial threats. Many of these techniques or measures may follow from existing best practice, rules or certifications, but for CL, the consequences may be as severe as when cybersecurity is breached in medical devices[98] or other areas which can damage individuals or human rights. What follows from this, is taking it gravely seriously, not only because of the consequences, but also the procedural risk that comes with it, as failures will warrant lawsuits of various kinds depending on the jurisdiction. On the other hand, if deployed outside of liberal democratic states, these considerations can be removed and CL can be used with impunity, as is seen in China[99], even if this is not advisable. Note that wording is soft, accommodate only indicates what is reasonable to expect, and does not mean that it cannot be merely resilient to the failures. As we noted earlier, resilience includes recovery, making a broader and inclusive wording more fitting.

Second recommendation. There are times where machine-learning[100] or other types of CL may not be adequate. *Firstly*, because manual decision-making or the existing judicial or public legal system is enough to handle to problem, or *secondarily*, because the proportionality or the consequences on rights or finances on individuals may weigh greater than implementing the system. Regardless of this, choosing to use CL is a political decision, but this recommendation then warrants *ex post* criticism and eventual dismantlement. There is little appreciation of the conservative aspect of non-choice or denial of certain uses of technology in existing rules, but this is traditional and well known in safety engineering. There will simply be times where safety risks outweigh the eventual advantages a system may bring, which means it should not be used, regardless of the financial or personal interests in it. This should in particular apply to CL because of its potentially systemic damage capabilities.

Third Recommendation. Mandating humans in systems is not in any way new, but we ask for it for a more traditional reason: The qualities which only humans have[101]. This is, again, a reference to the role which humans have in safety engineering, where our ability to adapt in emergencies make us invaluable[102]. Of course, the caveat to this is where adversarial behaviour or sludg-

[98] We discuss the potential consequences and attacks on medical devices like surgical robots in Ludvigsen and Nagaraja, "Dissecting liabilities in adversarial surgical robot failures: A national (Danish) and EU law perspective" (n 10).

[99] Fan Liang and Yuchen Chen, "The making of "good" citizens: China's Social Credit Systems and infrastructures of social quantification" (2022) 14(1) Policy and Internet 114.

[100] Isabel Chien and others, "Multi-disciplinary fairness considerations in machine learning for clinical trials" [2022] 906 ⟨http://arxiv.org/abs/2205.08875⟩.

[101] But it may have negative consequences, if used in a manner to circumvent or otherwise abuse the good ideas behind human oversight, see Ben Green, "The flaws of policies requiring human oversight of government algorithms" (2022) 45 Computer Law & Security Review 105681 ⟨https://doi.org/10.1016/j.clsr.2022.105681⟩.

[102] Leveson (n 29) 101 - 102.

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act' submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

ing[103] causes us to not react appropriately. Still, humans must act as both emergency measures and redundancies, the latter specifically referring to humans stepping in and overtaking the role which CL had so far. This could be in decision-making or automated assistance, both fields where humans used to sit, which means we still have experience and infrastructure to provide it, albeit much slower than what CL can provide. Article 14 in EU's proposed AI Act is a great example of how such a rule could be designed.

6 Future Work

Continuous in-depth analysis of existing CL systems, and acknowledging what constitutes CL to include as much as possible is, in our view, warranted. This should include interdisciplinary aspects, as understanding one side or another is not sufficient to actually comprehend the system as a whole, consequences, constraints and all.

The role which economics play in both enforcement or lobbying by powerful corporations or other states should be considered regarding CL too. Essentially, economic studies which critically consider the potential loopholes and adversarial actions that powerful actors can use against CL systems, is wanted on the basis of this paper, perhaps extending existing economics of security ideas.

Based on our very informal recommendations, expanded analysis on what constitutes the right situation to deploy CL, a condensed analysis of which threats for which types of CL exist, and the necessary human roles needed in CL would be adequate.

And finally, fusing CL research with existing but much older digitalised law[104] and legal informatics is suitable, as both fields have common agendas and perceptions of digital law, and would benefit from the expertise and alternative starting points which each bring.

[103] Much great literature exists on this, see Laura A Paul and others, "Teaching and Educational Methods Nudge or Sludge ? An In-Class Experimental Auction Illustrating How Misunderstood Scientific Information Can Change Consumer Behavior 1 Introduction and Background" (2022) 4(1) Applied Economics Teaching Resources (AETR) 34, for a recent overview and example.

[104] Such as the works by Jon Bing.

7 Conclusion

As it is clear, CL presents a situation where law gains both the advantages and disadvantages of the other discipline which inspired its existence[105]. In this paper, we firstly made a conceptualisation of cybersecurity in CL specifically, which consists of five levels. Now that CL absorbs cybersecurity weaknesses which occur in each layer, we show that there exists mitigation measures for the problems. But we know from safety and security engineering, that an ongoing arms race is and will be needed going forward, a sort of constant ongoing development of defences and considerations, which attempts to mitigate or lessen the damage that attacks can cause. Building these into CL will be vital, just as it is with cybersecurity everywhere else.

We find that CL is vulnerable to the same issues which both AI and neural networks face, if the systems make use of the technology[106]. The logic and practical implementation in which CL is implemented, presents a danger which very few other legal disciplines contain. Thereafter, we show how fragmented and rather softly cybersecurity is regulated in the EU, which in relation to CL, presents practical and real problems. But, we then analyse the AI Act, and it provides sound measures known from elsewhere regarding cybersecurity and human oversight. Regardless of issues with enforcement, this illustrates promise and understanding for a future where CL will play a central role in the legal system and in public consciousness in general. Clearly, the AI Act here combines CL (as AI) and cybersecurity, and regulates them together in a legal sense. Finally, we provide three recommendations for CL related to cybersecurity, which summarised are: Accommodation of threats, adequate use of CL, maintenance of the human role.

These are general, but from a EU perspective, the AI Act already does a good job in implementing them all, giving us hope for a future where CL and cybersecurity

[105] Not unlike the issues which philosophy or political directions has caused of systemic damage to law in the past. An example of this could be "communist law", see e.g., Jiří Přibáň, "From 'which rule of law?' to 'the rule of which law?': Post-communist experiences of european legal integration" (2009) 1(2) Hague Journal on the Rule of Law 337.

[106] This may seem rather redundant to mention, but these tend to be overlooked in favour of what advantages the systems may bring. In this sense, making sure that all aspects of new technology are discussed and understood is a core role of researchers and the public alike.

can safely melt together.

This is a pre-print entitled 'The dangers of computational law and cybersecurity; perspectives from engineering and the AI Act'
submitted to arXiv.org on 1 July 2022 - DOI: 10.48550/arXiv.2207.00295

Figure 1: Visualisation of the 5 weakness levels and their interactions.