Dissecting liabilities in adversarial surgical robot failures: A national (Danish) and European law perspective

K. Rosager Ludvigsen[1] and Shishir Nagaraja[2]

[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

July 2020

Abstract

Over the last decades, surgical robots have risen in prominence and usage. They are not merely tools, but have also become advanced instruments and have gained network connectivity. Being connected to a network exposes the robot to cyberattacks, which can damage the patient or the operator. These injuries are normally caused by safety failures, such as accidents with industrial robots, but cyberattacks are caused by security defects instead. Surgical robots are increasingly sold and used in the European Union, so we decide to uncover whether this change has been considered by European Union law, and which legal remedies and actions a patient or manufacturer would have in a single national legal system in the union.

We first conduct a case study, where we analyse which legal remedies a patient can make use of, if they are injured by a surgical robot caused by a cyberattack in the national legal system. We also explore whether cybersecurity and cyberattacks are considered by the upcoming Medical Device Regulation of the European Union.

We show that the selected national legal system is adequate to deal with this type of incident. This is because of its flexibility and in a certain approach even to ignore the distinction between safety and security to the benefit of the patient, and in one situation to remove liability from the manufacturer by nullifying its status as party. Otherwise, unless the operator or other parties have made the cyberattack more likely to occur, the manufacturer is liable.

We find that the regulation does not directly consider security defects, requiring interpretation and use of guidance to show it. Considering the real risk cyberattacks pose on medical equipment, we find this to not be adequate. We further find that the regulators of medical devices, including surgical robots, will not necessarily have adequate staff or rules of enforcement, as this has been left to the member states to solve. But, we also find, due to the comprehensive amount of rules that can be applied cumulatively, together with the possibility for further rules and compliance later on, that these issues could be solved in the future.

1 Introduction

In a world with an increased use of robot technology, surgeons are not the only ones whose hands are used operate on patients. Surgical robots are here as well, and offer assistance and unique approaches to treatment not possible before, with minimally invasive surgery being the primary technique. Two examples would be laparascopy done by the da Vinci systems[1] and the Magellan system being used for cardiosurgery[2] (Bergeles and Yang 2014). Surgical robots are widely used for a range of treatments (Holder, Khurana, Harrison, et al. 2016), for example for hernia and intestinal cancer[3].

The surgeon and the patient are not the only relevant parties when it comes to the surgical robots. Engineers, programmers, nurses, lawyers and a whole range of other staff are needed during the design, production, operation and maintenance of them, and if accidents happen to the patient or people surrounding it. This also applies to the research, and keeping up with the developments in both the technical, healthcare and legal sphere is difficult, which is why guidance on it always needed.

Surgical robots are increasingly sold and used in the European Union, which means that both its legal framework as well as those in each member state apply to them.

We will therefore apply both European Law and national law, in this case Danish law, to the issues that cyberattacks on surgical robots that lead to injuries present. This gives us the overarching picture for manufacturers in the union, as well as the in depth perspective on when the cyberattack is successful, and someone has to cover the damages done to the patient.

Surgical robots are considered cyberphysical systems (CPS), because they are robots that interface with the physical world, with their tools being used directly on the patient. The risk of injury or damage caused by the robot, due to internal failure or deterioration is called safety, for both patient or anyone else surrounding the robot. Safety failures can lead to injury, but cyberattacks from individuals or organizations outside of the hospital are now able to as well[4]. We can express this as security defects causing safety complications. This is a constant threat as such attacks change and come from many angles.

We will not answer how the attacks can be prevented, but approaching the issue from a practical point of view is maintained. These cyberattacks and security issues are prevented with legal frameworks, and when injury occurs, remedies within law exist to mend the damage caused. While most literature mention the possibility of this, we take a closer look at some of the issues these situations would present in a national court, as well as the rules concerning the prevention on a European level.

---

[1]Operation by small incisions into abdomen or pelvis with the aid of a camera.

[2]Surgery on the heart and great vessels.

[3]A da Vinci surgical robot from a small Danish hospital broke the record with 426 performed surgeries in 2019, and it is mainly used for said treatments.

[4]Such as unwanted movement of tools inside the patient, or the machine stopping entirely (Alemzadeh, Chen, et al. 2016)

We therefore ask how these robots are regulated at an European Union level, and whether the rules consider the cybersecurity aspect. We would also like to know how an accident involving a cyberattack is considered from the patient's point of view within a national legal system, to keep it as pragmatic as possible.

Connected surgical robots are considered medical devices, which means they are to be regulated by the European Medical Device Regulation (hereafter the Medical Device Regulation), 2017/745, since they fit the definition of "medical devices for human use" seen in article[5] 1(1)[6].

The legal remedies that we analyse to gain compensation for injuries caused by a cyberattack on a surgical robot in Danish law are: Product liability and reimbursement outside of contract lawsuits, and a "Patient Reimbursement" case.

The paper is built up as follows: We define surgical robots, adversarial failures and adversaries in section 2. On the basis of these definitions, we analyze whether the three different legal remedies in Danish law, that can be used to recover damages from a cyberattack on a connected surgical robot are possible to use in practice in section 3. In the same context, we identify and try to uncover whether and how the future Medical Device Regulation from EU-law handle the same issues and cybersecurity in regards to surgical robots in section 4. We quickly discuss the NIS Directives relevance in regards to the topic in section 5. In section 6 we try to extract principles that can used for other jurisdictions from our analysis, and in section 7 we take a short look at related and future work, with concluding remarks in section 8.

We find that seeking compensation with product liability in Danish law is likely. A lawsuit based on reimbursement outside of contract is likely as well, but proving the link between careless behaviour and the injury can be difficult. An administrative case in Patient Reimbursement system is very possible however, because it disregards the nature of the cyberattacks, and merely requires that it is proven that the surgical robot "fails". Overall, we see that even if a cyberattack is difficult to prove, the approach of the Patient Reimbursement, the flexibility of the Reimbursement outside of contract and the idea of defects allow patients to recover damages in practice.

We also find that the Medical Device Regulation does not literally address the cybersecurity issues that both surgical robots and other devices gain from network connectivity. They can be interpreted to be included with help from guidance on cybersecurity, but because the rules are not explicit, there is a risk that the threats to patient health are not prioritized. We find that the lack of explicit oversight concerning cybersecurity occur to the regulators[7] as well, which raises doubts whether security compliance can be enforced.

---

[5]Abbreviated to art.

[6]This regulation was postponed with a year to 26/05/2021.

[7]National authorities that oversee compliance, see art. 101.

Scope of this paper: In law, we work with subjects, which here consist of manufacturers and regulators, who act on the medical devices as such, and the opposing subject of the patient. We exclude importers, distributors and others that have special rules, since they will not affect the cybersecurity of surgical robots.[8] This paper will not consider the same issues with the Medical Device Directive, or regulation 2017/746 on in vitro diagnostic medical devices[9]. Furthermore, we choose not to include untethered microsurgeons in our analysis, even if they are closely related to surgical robots as such. Finally, we do not discuss the interactions between the NIS directive[10] and Danish or EU-law until section 5.

2 Definitions

In this section we define what connected surgical robots are, how they are considered cyberphysical systems, what adversarial and non-adversarial failures are, and which adversaries would try to induce these failures.

2.1 Surgical Robots

The two terms active surgical robotics and telerobotics are closely related and generally explain what we see as surgical robots (Hockstein et al. 2007) (Bergeles and Yang 2014). Active surgical robotics means robots with pre-programmed data and computer-generated algorithms that function without real-time operator input (Hockstein et al. 2007).[11] While also containing these features, telerobotics additionally emphasizes a remote control of a robot by a human. Control of the robot can be completely manual, or supervisory, the latter requiring substantial intelligence and/or autonomy for the robot (Niemeyer, Preusche, and Hirzinger 2008). A telerobotic system has an operator-site and a remote-site. The operator-site usually has an acoustic display, a visual display, a tactile display and a haptic display. Remote-site usually has acoustic/visual haptic/kinesthetic-tactile sensors or actuators (Niemeyer, Preusche, and Hirzinger 2008). For this paper, we focus on telerobotics, which we will merely call connected surgical robots, since they require a network connection to function properly.

---

[8] Unless they install/change the software on the devices.

[9] Which has not been postponed, and may include specific surgical robots.

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

[11] An example of the first generation of actual robotic surgical systems, could be the experimental PUMA 200 manipulator from 1988, which would define entry orientation and location of a surgical needle. The operator would then insert the needle as defined by the robot (Bergeles and Yang 2014).

2.2 Cyberphysical Systems

As mentioned, connected surgical robots are cyberphysical systems (CPS), which means they seamlessly integrate computation and physical components into their operation (NSF 2014). A generic description would be: the lowest level starts with sensors and actuators, which are connected to a field or a sensor network, all of which would be managed by a control system, that itself would be bound to a control system network (Kobara 2016). The human machine interface would exist at this level, which would be where the operator of a surgical robot would reside. Autonomous cars, smart grids and IoT devices all fit these criteria, but with these features come many vulnerabilities, which are included with the connection to a network or the internet. As they have physical components, these devices can interact and affect the health of humans, and so can an adversary that successfully attacks the system. This shows that connected surgical robots, in this context, can be considered safety-critical systems, because of the potential risks imposed on the patient (Alemzadeh, Raman, et al. 2016).

CPS consists of many hardware and software systems combined, and each can be manipulated from the outside, even if it is loosely isolated from the internet (Kobara 2016). To put this into perspective, from 2000 to 2013, 144 deaths caused by adverse effects related to surgical robotic operations were reported in the US (Barry et al. 2012).[12]

2.3 Adversarial failures

Given the extensive developments in CPS, we can assume it is hard for manufacturers, doctors, hospitals, robot operators, engineers, lawyers, and policymakers to keep up with the developments in the world of these systems. However, as these solutions become popular, there is ever greater need to understand how they fail, since this is fundamental to any litigation and assignment of responsibility. Any action that is intentional and seeks to induce failure, is considered a cyberattack. In this context, we decide to classify failures as primarily adversarial and non-adversarial failures. Failures refer to what the cybersecurity system fails to prevent.

Adversarial failures are caused by an active adversary who attempts to induce failures to attain their goals, such as manipulating the surgeon's commands, inferring the surgical procedure to compromise patient privacy, or the theft of intellectual property such as the robot's algorithm or trade-sensitive data like the surgeon's inputs. There exists other taxonomies for security (Rizvi et al. 2018) (Quarta et al. 2017) (Papp, Ma, and Buttyan 2015) (Aslam, Krsul, and Spafford 1996) (Al. 1994) and safety (Vasic and Billard 2013), but we feel that a separate taxonomy is needed, due to the specific issues that connected surgical robots pose. Our proposed categories of adversarial failures for connected surgical robots are as follows:

1. Manipulation Attacks. The adversary covertly modifies the instructions to

---

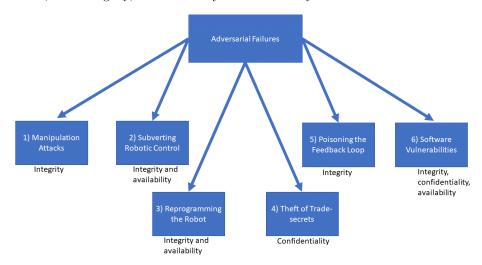[12]None of these were caused by cyberattacks, as far as we know.

get a different desired response. This is understood in the broadest sense, since it can be initiated in any part of the CPS that connected surgical robots consist of. This was tested in practice on the RAVEN II open platform, which is similar to current connected surgical robots(Alemzadeh, Chen, et al. 2016). The attacks were injections of unintended user inputs, or motor torque commands, which required access to the master console or control software. The effect of this failure would be unintended jumps, movements or for the robot to completely stop.

2. Subverting robotic control. The adversary hijacks or otherwise makes changes in the robot's control. This is different from manipulation, since this can be done on the network the robot receives signals from, and focuses on the control, not manipulating existing actions. A practical test worth mentioning, done on the same connected surgical robotic platform as before(Bonaci et al. 2015), where packets were delayed or changed between the operator and robot, and using this technique, they were also able to hijack the surgical robot[13]. While the first two can only cause delays in movements, the latter completely enables the adversary to do as they please, potentially harming the patient.

3. Reprogramming the robot. The type of access that is needed to manipulate the robot, may also allow access to change the software as well. The failure consists of changes in software on any level, and while we do not have practical examples for connected surgical robots, the severity of such failures on the patient or operation in general is large enough to raise concern. The possible enabling of other failures or other newly programmed actions are great, and this only shows how important maintenance and routine validation of equipment is.

4. Theft of trade-secrets. This is seen as the attackers recreating the underlying technique of surgery by collecting surgical control instructions over time. This failure can be done initiated over the network or inside the surgical robot. While it cannot harm the patient, it is theft of the techniques used by surgeons currently, and could in the future constitute the basis for data sets that AI or machine learning algorithms can use to replace the operator entirely. Collecting this without the consent of the surgeon is both unethical and most likely violates rules on trade-secrets, and it constitutes an issue that will generally need to be addressed further on.

5. Poisoning the feedback loop. The adversary covertly modifies the camera and/or other sensory outputs sent to the surgeon. Sensory inputs are currently vital for showing where the procedure inside the patient is at, as well as what the surgeon is currently doing. If any of these are changed, the

---

[13]This was done by fooling the robot to believe that input believing packet loss was occurring, but not enough to interrupt the operation, and it would then only be able to be controlled by the packets sent by the adversary.

risk of injury of the patient increases. The difficulty of resetting or returning the robot to its initial position is further hampered by any feedback being off or wrong, which makes this a dangerous failure.

6. Software vulnerabilities. Any vulnerability that an adversary can make use of to commit further attacks on, is considered a failure as such. It is also the broadest, since it covers any part of the connected surgical robot and its accessories. Unlikely the failures above, this is passive and not necessarily caused by the adversary, but instead enables them to cause failures because of it.

Figure 1: Illustration of Adversarial failures, which includes what is compromised, here integrity, confidentiality and availability.

2.3.1 Non-adversarial failures

We do not discuss non-adversarial failures in this paper, but we choose to list them for completeness. Non-adversarial failures are caused by the correct operation of the robots as per the specification, but where an unsafe outcome is caused nonetheless. We see them as:

1. The robot works in unintended ways because of failures in motor calibration or sensory defects.

2. The robot causes a denial of service on itself whilst legitimately trying to accomplish the assigned task.

3. The robot has an incremental bias which creeps in due to shifts in belt tensions, gear wear-and-tear and other electro-mechanical reasons.

4. The robot fails to handle shifts in lighting, shadows, tilt of surface level, noise, mist or other environmental noise in the visual or acoustic plane.

5. The robot fails to perform due to inability to function in poor network conditions or being operated in network conditions (jitter, throughput, and bandwidth) that are quite different from what it was tested on.

2.4 Adversarial model

The identity of the adversary, the party that seeks to cause adversarial failures, have different priorities and focuses, so we have decided to assume certain things about them. Adversaries are traditionally modelled.

Our adversarial model includes cybercriminals, disgruntled employees, terrorists/activists/organized criminal groups, and nation states (Cardenas 2009), as well as competing surgical robot manufacturers. We choose to have the widest range of actors possible, since the choice of them and which failure they want to induce, can change the outcome of the analysis in the following sections.

As shown, we assume that stronger players can induce many failures, while competitors and disgruntled employees would only do a few. We leave out any attacks that can cause injury from those two, since none of them would have the intention to cause them in the first place. Cybercriminals and organized criminals groups overlap, and can generally both create all failures except for software vulnerabilities, but we assume that theft of trade-secrets would be done only by the organized party. Terrorists/activists would want to create as much of an uproar as possible, which is why they would go for failures that cause this. And nation states are capable of everything, with the highest amount of resources at their disposal.

2.5 Legal Sources

In the next sections, we make use of a range of legislation and regulations.

Figure 2: Illustration of which adversarial failures the adversaries make use of.

Adversaries / Adversarial failures	Cybercriminals	Disgruntled Employees	Terrorists/activists	Nation States	Competitors	Organized Criminal Groups
Manipulation Attacks	X		X	X		X
Subverting Robotic Control	X		X	X		X
Reprogramming the Robot	X		X	X		X
Theft of Trade-secrets		X		X	X	X
Poisoning the Feedback Loop	X		X	X		X
Software Vulnerabilities				X	X	

Since connected surgical robots are sold both at a national and European level, we include the overarching rules as well as national rules for litigation.

The Danish legislation includes rules for suing manufacturers, as well as law for public authorities since one approach to compensation is through an administrative system.

2.5.1   EU-law

Directive 85/374/EEC on product liability, directive 93/42/EEC on medical devices, regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters, directive 2016/1148 (the NIS Directive), regulation 2017/745 on medical devices and regulation 2020/561 on amending regulation on medical devices, as regards the dates of application of certain of its provisions.

2.5.2   Danish Law

Law of product liability[14], law of public administration[15], law of healthcare[16], law on medicinal equipment[17], the NIS law[18], and the act of complaint and reimbursement access in the healthcare sector[19].

---

[14]LBK nr. 261, 20/03/2007, notation for Danish law.
[15]LBK nr. 995, 22/04/2014.
[16]LBK nr. 433, 22/04/2014.
[17]LBK nr. 139, 15/02/2016.
[18]LOV nr. 436, 08/05/2018.
[19]LBK nr. 995, 14/06/2018

3 Case: Danish law

In the following section we show how patients can use applicable law to recover their damages from a cyberattack on a connected surgical robot. We show whether a lawsuit with product liability, reimbursement outside of contract or a case in the Patient Reimbursement system in Danish law will be likely to succeed, and we do so from the perspective of the patient as the claimant, and the manufacturer as the defendant.

3.0.1 Initial comments

Robots as such in Danish law do not have *lex specialis*[20] made for them, and outside the implementation of the NIS directive cybersecurity and cyberattacks do not have any either. Directives are implemented into national law, not directly used like regulations, see art. 288 in the TEU[21].

Before one makes use of the most general approach to compensation, two other types must be considered, as these are *lex specialis*, albeit not for cyberattacks or cybersecurity. We therefore go through product liability, then patient reimbursement below.

However, both specialized approaches build on the thoughts from reimbursement outside of contract. This type of lawsuit is based on case law. The patient can always fall back on this, if the others are deemed to have a low chance to succeed. This type of lawsuit requires that 4 specific case law based criteria for reimbursement are fulfilled: someone who is liable, quantifiable damage, a link between the responsible and the damage and that the link is adequate (Eyben and Isager 2013). These have to be fulfilled cumulatively, and in order. The defendant may have acted carelessly, and the adversarial failure caused damage, and a link between the two is made likely, but if the link is not adequate, the cased will be ruled in favour of the defendant. We will come back to this last approach after the other two.

Both the lawsuits will be part of civil litigation, which initially leaves the patient at a disadvantage in terms of providing evidence. But this changes as we will show below.

3.1 Product liability

If a product is defective, and causes damage, a lawsuit on the basis of product liability can be initiated. Defect is defined as the product being less safe than a person is entitled to expect[22].

If a patient being treated by a medical device that fails due to a defect and gets injured, we know that the patient is entitled to directly sue the manufacturer instead of the hospital in Danish law. This was answered more than forty

---

[20]Specialized legislation.
[21]Treaty of the Functioning of the European Union.
[22]See art. 1 in the Product Liability Directive, or § 5 in the implementation law.

years ago in the case U.1960.576H[23], where two patients kept the manufacturer of oxygen machines liable for the damage that was caused on them as they were hospitalized.

Product liability can be sought in three ways in Danish law. The first is on the basis of the product liability directive, the second is through a case law based approach that existed before the directive[24], and the third is the oldest and is product liability through contract.

3.1.1 Product liability directive lawsuit

Lawsuits for product liability are usually initiated on the basis of the Product Liability Directive in Danish law (Andersen and Lookofsky 2010). Since it is a directive, it has to be implemented into Danish law, which was done with the law of product liability. We therefore refer to the relevant paragraphs therein.

First, we see that the surgical robot and accessories are included by the law, see § 3.

Secondly, we must consider whether the manufacturer is exempted from responsibility. Connected surgical robots that are not considered goods are exempted, see § 3. This refers to idiosyncratic surgical robots that cannot be moved without destroying them. The defendant can further argue, that if the surgical robot has not been put into circulation, has been designed to be used by a single hospital, or that due to the state of the art the time it was impossible to discover the defect, they are not responsible, see § 7, part 1. The last is especially important, since this enables the defendant to argue against any adversarial failures caused by new or unusual means, but the burden of proof for this is incredibly high, as it is the knowledge of the entire industry, not just what the single manufacturer knew at the time.

If none of these apply, we go through the rest of the process. The burden of proof is on the claimant, who would have to prove that a defect exists, see § 6. They also have to prove the damage as well as the link between the defect and the damage. The responsibility is objectively on the manufacturer. A defect is defined as the product being less safe than a person is entitled to expect, and the patient would claim that they can expect for the surgery to only fail due to mistakes by the operator or mechanical or safety failures. Three considerations can modify this assessment, which are the marketing of the product, its intended and expected use and the time at which it was put into circulation, see § 5, part 1. Marketing is irrelevant to this claimant, but intended and expected use will include some unusual considerations when it comes to the last exemption from § 7. Since the use of such a robot naturally will include maintenance of any level of software, the idea of release of the product into circulation becomes void, when considering cybersecurity aspects, unless it is impossible to defend against, without designing new products, such as adversarial failures caused by quantum computing.

---

[23]Notation for Danish case law.

[24]Also called delict based product liability.

Identifying the defect is crucial, which would require that the claimant obtains proof of the three adversarial failures that potentially can cause an injury on the patient. These are manipulation attacks, subversion of robotic control and poisoning of the feedback loop. We will continue to use these further down as well. They could require original design documentation, which an expert witness could show would risk specific manipulation of the robot or subversion of the control of the robot over the network, as well as poisoning of the feedback loop given from visual and haptic sources. Another approach, which is even more appropriate, is *res ipse loquitur*[25], proving that the injury was not caused by human or other error. This would force the defendant to either argue that it was caused by a safety defect, which would make no difference for the injured party other than a new lawsuit, or make them argue why the failure had not happened. The claimant would then claim that since it could never be caused by human error or a safety defect, it must have been a defect that the defendant is responsible for. Since this is a civil lawsuit, in the situation where the defendant decides to deny all claims and not argue, the claimant is likely to succeed, as silence on the matter speaks against the defendant, considering the severity of the damage which is human injury. This is further supported by the role this and reimbursement outside of contract lawsuits present, since they would be used in situations without insurance.

The claimant would then have to prove the damage had occurred, which we assume they are able to, but they would also have to prove the link between the defect and it.[26]. The claimant can choose to argue for a direct or indirect link. For the link to be direct, it has to be physically seen or decipherable from log files. For it to be indirect, it has to be derivable from the situation. We have two cases that illustrate the duality of the indirect link. Lawsuits from the case law based approach are free to be used in the directive based approach, even if the legal sources for it are different.

In the case U.1939.16H, cattle owned by the claimant died after being fed black treacle. Out of a set amount of cattle, only those fed with the black treacle produced by the defendant died the following week. The claimant claimed, after having used an expert witness that showed that they were at good health before being poisoned, that they had not been overfed or otherwise damaged by the claimant, that the cattle which were not fed with it survived, and that poisoning from the black treacle could therefore be the only cause of death. The argument was built so because a vet at the time could not clinically prove it, which is why the link is indirect. Black treacle acts as supplement, and is not supposed to have any drawbacks. The defendant argued, that the claimant had not proven this sufficiently, but did not provide additional reasoning for why this was so. The Danish Supreme Court found, that there could be no other reason for the deaths occurring, and followed through with the claims of the claimant. This case is referenced frequently, and has a high level of authority.

In the case U.2003.1706H, the claimant's roses that were fed with peat man-

---

[25]Elimination of other factors than the one you want to indirectly prove caused it.

[26]The link as we see it here, is not the same as the one in reimbursement outside of contract.

ufactured by the defendant experienced distorted growth. The parties agreed, that the distorted growth was caused by oxygen deprivation. An expert witness brought by the defendant made it clear, that the contents of the peat were fit for use. The claimant used same argumentation as from above, that is, that due to the circumstances, the peat causing it is the only plausible outcome. Supreme Court found that just because the distorted growth stopped after a change in peat, did not mean that the peat caused it, nor that the peat could have been different than how it was described, and that the peat was not different than what was previously agreed and delivered between the parties. This case has a high level of authority as well, while it shows the opposite situation from before.

If we apply case law, we see that unless the claimant has access to log files that show adversarial failure, and/or design documentation that shows which defences and adversarial failures that were considered, the claimant should try to argue for an indirect link. They are likely to succeed with this, since the concept of the same product suddenly having a defect, the argument from the second case, does not apply to adversarial failures that are caused by inadequate defences.

The defendant has another case law based tool they can make use of, which is the test for whether the defect is "systemic damage" (Andersen and Lookofsky 2010), which if true, shows that the product cannot be considered defective. The distinction between danger and defect is explained below, but has no effect on the test. The defendant would have to build their procedure around the test being fulfilled, which equates to two questions answered with a yes. These are:

- Are the dangers known? The danger of manipulation attacks, subversion of robotic control and poisoning of the feedback are all known, but they are not necessarily known for each type of connected surgical robot. It has be known for the product. The claimant would claim, that they are not known and ask for documentation for this otherwise. The defendant would argue, that the underlying risk of any type of cyberattack, warrants public knowledge of the dangers. But the defendant is unlikely to prove anything with such a general argument, since it is product specific. We know from case law, especially from U.2015.572H[27], that known refers to the product only, and any vague statements are not accepted by the judges.

- Are the dangers unavoidable? By unavoidable, it refers to whether the scientific and technical community deems these to be so. The defendant would claim, that all adversarial failures are generally unavoidable because of new techniques and vulnerabilities. The argument of constant development would be used. The claimant would retort to this, that certain adversarial failures are more preventable than others. The exception

---

[27]Groundbreaking case, where a claimant tried to sue the manufacturer of a big tobacco brand for the cancer that the excessive use of cigarettes had caused. They failed, because the damage caused to her was considered systemic, because it was both known by everyone concerning the product, and unavoidable if you smoked it.

would generally be subversion of robotic control. The exception is there, because the manufacturer cannot perfectly control the network that the connected surgical robot receives commands over. They are however able to build suitable defences against the rest, even if doing so in CPS is difficult.

It is unlikely that both questions in this test can be answered with yes, since the public at large does not know that these adversarial failures can occur to connected surgical robots, but certain adversarial failures may be considered unavoidable. Most importantly, the judges have to be convinced of this, and even if both could be answered with a yes, that does not mean that the judges will decide to allow the test.

3.1.2 Product liability lawsuit via case law

Initially, it has to be mentioned that The European Court of Justice (ECJ) has concluded, that this approach can only be used where the product liability directive does not apply, see for example case C-183/00[28] where a Spanish set of product liability rules that put the patient/consumers in a more favorable position, was ruled to violate the directive (Andersen and Lookofsky 2010). This means that this approach can only be used on connected surgical robots, that are not covered by the directive, see § 3 from the law of product liability. In practice this would limit it to completely custom made surgical robots, as well as those that cannot be moved without being destroyed.

While the test of systemic damage, and the use of case law from earlier, still apply to this approach, there are certain differences in how the defect is defined. Both the definition of defect from above can be used, as well as the old term "danger" (Andersen and Lookofsky 2010). If the product can injure user or third person, it is considered dangerous. But to be defective, it has to be "unreasonably dangerous".

This implies that some products are inherently dangerous to use, but it is the manner of danger outside of this that determine it. A good analogy would be candy, it is not unreasonably dangerous that excessive consumption makes you fat. Any software system or device that is connected to the internet or local network, pose a direct danger to the patient due to the known vulnerabilities and possibilities of abuse it contains. But for it to be unreasonable, it has to have a risk to occur often or commonly, which so far seems to not be the case here.

We also notice that many other legal areas neglect to identify and see adversarial failures as unreasonably dangerous in Danish law, which further supports that it is not. The use of 'defect' from the directive is therefore appropriate, since unreasonably danger would not cover adversarial failures, and because the terms can be used interchangeably in both approaches.

Otherwise, the case would proceed as above depending on the adversarial failure that is possible to prove or imply by the claimant.

---

[28]Notation for case law from the ECJ.

3.1.3 Lawsuit on product liability in contract based on case law

The contractual approach is next. It is also based off case law. If possible, this type of lawsuit would completely circumvent the rules laid out above, and instead merely focus on analogies to the Danish law of purchases, which would lead to cases where the evaluation of the sale of a proper product was met or not. This would apply to the patient as a third party, and allow a lawsuit. To make use of this, the claimant must first prove that there exists a contract between them and the operator or manufacturer. Clearly, the patient has not signed anything with either in written form, but has the patient done so orally? To assume the patient has accepted an oral contract with the hospital or the doctor, there has to be a so called "meeting of the minds" (Gomard, Godsk Pedersen, and Ørgaard 2015) in Danish law. Such a meeting must here include the accept of treatment being done in part or partially by a surgical robot, and the general risk of failure of the machine or anaesthetics. Whether they have to disclose the risk of adversarial failures is unlikely, since there have been recorded 0 of them on surgical robots in Denmark. However, the claimant is not likely to prove that this exists, since Danish healthcare law does not work with contracts between these two parties in the context of private law. This means that the judge would dismiss the case on the basis of a lack of a contract.

3.1.4 Comments on Evidencing

Like expressed above, proving that the defect exists in the product, and whether the link exists between the defect and the injury are complicated for the claimant. Initially, they do not posses the necessary design documentation or files that show, that the adversarial failure caused their injury. Like in other cases, they can show that nothing else could have caused the failure, such as expert witnesses or even the operators that worked with the robot at the time, or system admins. This would force the defendant has to provide some of documentation directly or otherwise face the its opponents claims unopposed.

Furthermore, the European Medical Device Regulation[29] has a special function in regards to proofs in these cases. In art. 10(14), paragraph 3, if the regulator determines damaged occurred, it can upon request transfer all documentation that it has access to the patient/representatives, requiring there being a public interest in disclosure to overrule any violation of data protection rights and without violating intellectual property rights. While this has not been used in practice, it more or less acts as a right for the patient. This can be used both here and in the lawsuit further down. The idea of intellectual property rights can be stretched far, which can practically limit the amount that can be shared. But since civil lawsuits in Danish law can be held behind closed doors, documentation that in an open case would violate those rights can be used, if deemed possible by the regulator. The court decides on whether it is appropriate, if contested by the defendant. Public interest refers to what it literally reads as, which means that it has to potentially affect more than the claimant,

---

[29]Regulation 2017/745.

or have consequences otherwise, which adversarial failures on connected surgical robots warrant.

3.2   Patient Reimbursement

The act of complaint and reimbursement access in the health-sector defines the structure and the requirements for patient reimbursement cases.

The means to do so is called "patient reimbursement", which is not a lawsuit, but instead an administrative way to receive compensation. This is facilitated by the Patient Reimbursement Authority[30], which is financed and run by the Danish state and private parties, and it solely considers and decides on cases in regards to patient injury[31]. It does so in the manner as any public authority would, via the principle of officiality[32] in Danish public law. It includes the collection of evidence by the authority if necessary, and perfect application of existing law and committing to the correct decision.

The patient applies for patient reimbursement on the authority's website. This means that in this case, the only parties are the patient and the state, since the subject of such cases can only be the one who initiates it, and the state is by default the one who compensates.

The objective liability for this damage rest on the regions that run the hospitals, which in practice means the state, see § 29.

The types of damages that are considered are laid out in § 20, part 1. Since it is not caused by the operator, the damage sustained has to be caused by "errors or failures in technical apparatus". Any type of failure, whether it was caused by neglect or other, are considered to be covered by this type of damage. The damage has to be caused "most likely" by the failure or neglect, see § 20 part 1. This is especially important, when the patient was considerably weakened, and the injury likely would not have caused any damage had they not been sick. The patient would here be advised to make sure, that the evidence necessary is seen by the authority. Otherwise, the only criterion would be, that the damage was more likely to be caused than not.

An adversarial failure induced by an adversary into these kinds of systems is possible, and an injury caused by it always establishes a link between the failure and the injury. But if the adversary is able to hide those details, the operator can still attest that the machine failed, so it would then go from a cybersecurity to a safety case, of which there is well established practice that supports the patient, as well as the literal reading of § 20, part 1.

After the application has been sent, the authority would then collect information from the hospital where the injury took place, including documentation created by the operator of the connected surgical robot. The patient is free to provide further evidence, but since the authority has responsibility to make the right decision, they do not need to. If they want to, the patient is able to

---

[30]Staff includes doctors and lawyers.

[31]See §§ 32 and 33 in the act.

[32]This principle is not codified, but seen in case law, literature and Ombudsmand's practice.

access[33] which documentation the authority base their decision on, and halt the process until they have provided further proof. But this is supposed to be the exception.

The decision can be appealed to the courts, or to the appeal board driven by the resort ministry[34].

The amount one is able to recover is comparable to a successful lawsuit, and applying for it is free. Only compensation for quantifiable damage and pain and suffering is possible, as the Danish definition of tort is not applicable here. If the patient accepts the judgement, and does not act further, they will receive the compensation at the date of the decision.

As long as the patient sustained quantifiable damage, and the connected surgical robot has sustained a failure, even if it cannot be proven to have been caused by an adversarial one, they are able to receive compensation.

But what if adversarial failures on surgical robots become commonplace? This could lead to this method not being possible, either because of a change in the act, or because the administrative practice would interpret its way out of it, such as assuming that adversarial failures would not qualify.

3.2.1   Comments on Evidencing

Proving it in the Patient Reimbursement environment is different, as seen with the influence of public law and the lack of court rules. Therefore, the full burden of proof does not lie on the patient, but on the authority. Since they merely need to decide on whether equipment encountered an error or failed, seeing the failure and damage occur would be sufficient. However, it is unlikely that they have individuals educated to read the logs that such adversarial failures will create, but they can require the hospital/manufacturer to explain this to them. Cooperation with the Danish regulator [35] is possible as well, since the sharing of documentation between such parties is allowed. They will have all documentation necessary for the surgical robots to be put into circulation on the European market.

In the next section, we go back to a lawsuit that is always possible to proceed but maybe not succeed.

3.3   Reimbursement Outside of Contract

The default for seeking compensation in Danish law, is reimbursement outside of law, where the four requirements, liability (through acts of carelessness), quantifiable damage, a link between the responsible and the damage and that the link is adequate have to be fulfilled. Unlike the examples above, there is no objective responsibility, only *culpa* which the manufacturer must have committed[36] (Eyben and Isager 2013).

---

[33]Equivalent to a Freedom of Information Request, or other national tools.

[34]Relevant ministerial organ, usually under the Minister of Health, but each government decides their own structure.

[35]The Danish Medicines Agency in this case.

[36]Which is translated into carelessness instead of negligence.

Traditionally the standard for what is not careless, is what a *bonus familias pater*[37] would do. However, this is criticized in Danish law (Eyben and Isager 2013)[38], and the standard is gradually moving towards a focus on the breach of rules (both legal and otherwise) or the "normal right to act". This is defined or at least elaborated on in case law, but it has not specifically been done for manufacturers of CPS.

3.3.1 Fulfillment of Criteria

For the lawsuit to be successful, the patient that was injured by a connected surgical because of an adversarial failure, has to make it likely for the court that the criteria mentioned earlier are fulfilled. The defendant will attempt to disprove this in various ways, which we will show below.

First, the claimant has to show that the defendant acted carelessly in relation to the adversarial failure. Like mentioned earlier, there does not exist *lex specialis* they can have broken here, which would normally be enough to show carelessness.

The claimant will not initially have any documentation concerning what considerations were taken about the prevention of adversarial failures in the company. But they can bring forth the argument, that the manufacturer failed to act to prevent the adversarial failure from occurring. This assumes this was made clear first, and if not, the claimant can say the same about the safety aspect that allowed the patient to be injured. The evaluation of carelessness is broad, so the claimant could also bring out the danger of a surgical robot, that warrants the utmost caution in both its design and later service given. The defendant can either choose to bring out the documentation that shows, that they did consider the one adversarial failure that caused the injury, but could also go for the approach where they do not reveal which one.

Like in product liability, this is a disadvantage, since silence or dismissal does not prove anything in a civil lawsuit[39]. Due to the severity of the injury and of the big risk it poses, as both the da Vinci and Magellan systems can cause internal hemorrhage, the barrier to show carelessness is further lowered. The final nail in the coffin would be the support of "responsibility based on profession" that is seen in case law regarding safety in this area (Eyben and Isager 2013). We can apply from safety to security, due to the consequences of it being the same.

In the case U.2010.1350H, the defendant had installed ventilation equipment at the address of the claimant, but a fire developed after the defendant had left the property. This had happened due to a known defect with smoke cartridges after the installation, and the defendant knew this both from sector and own experience. The judge concluded, that because of this knowledge and because they are considered professionals in the business, they acted carelessly and were

---

[37]Translates to the ideal family dad.
[38]Defended by Langbo, Lars Bo in a specific context, but the reasoning is as easily reached by not using the term.
[39]Unless the claims are unreasonable or out of proportion.

therefore responsible[40]. Had this been between two consumers, the act would not have been considered careless. In a security context, this means that if it is known that manipulation attacks, subversion of robotic control and poisoning of the feedback loop is possible, any professional must make all attempts to prevent it, and must prove they have done so, as to not be kept liable. The claimant is therefore likely to be able to fulfill this criteria.

Another clear way to show carelessness is to have violated or otherwise not complied with rules put down in law. Even if the case is not about personal data, if the defendant had breached this as well, the bar for proving what is mentioned is mentioned is further lowered, but not entirely clear if there had been *lex specialis* to breach. On the other hand, the defendant could bring out the argument, that a third party had not complied with cybersecurity legislation such as the NIS directive. They would have to prove, that if the breach of cybersecurity by the hospital, caused the adversarial failure or made much more likely, they would not liable. If this was the case, such a lawsuit would require the claimant, after having a verdict going against them to sue the operator (hospital) of the surgical robot instead.

We assume that any injury sustained is quantifiable, which means that the second criterion is fulfilled. The claimant would need reports from hospital staff and could also get a second opinion on the injury. This will be contested by the defendant, who might bring an expert witness, to scrutinize the documentation provided by the claimant, but this is rarely worth the costs.

The next issue becomes whether there is a link between the careless behaviour and the injury. The claimant has to prove, that the careless behaviour directly or indirectly likely caused the damage. Like in product liability, this is usually the most difficult part for the claimant to prove in a lawsuit, but their use of the term differ. In reimbursement outside of contract, the claimant merely has to make it more than likely, that the carelessness caused the damage.

The defendant can attempt to prove, that the injury would have occurred no matter what they had done, which brings us back to the different adversarial failures. If the failure is subversion of robotic control, there are situations where the manufacturer could not have implemented defences that could have prevented it. In that situation, it would only be the network administrator and therefore the hospital, that could have prevented it, which makes the claimant unlikely to succeed. But in regards to the other two, the claimant can argue that the chance of the adversarial failure occurring would have been lower, had the defendant actively attempted to prevent it.

The defendant can retort, that the injury would have occurred regardless of their behaviour. This is related to the idea of *conditio sine qua non*[41], where the act of carelessness must have made it more than likely for the injury to occur. To do this, they would have the prove that the adversarial failure was impossible to prevent, therefore making the link impossible to prove for the claimant. But the burden to prove this is very high.

---

[40]We do not make use of the rest of the case.

[41]A requirement, without it none is possible.

The defendant can bring a tangential issue out, which is whether there are competing causes for the damage. They can argue, that there always exists a risk for an adversary to cause an adversarial failure, regardless of their mistake, for example caused by the failure of software vulnerabilities in generic operating systems on their devices. But the defendant would again need to prove this, and vague general statements about "technical advancements" and "new techniques" from hackers are too vague, and do not constitute a competing cause. Even if they can prove, that an update of software they do control caused the failure, this does not equate to the judge supporting the argument, nor does it refute the compelling argument made by the claimant.

A piece of safety case law can further show how complicated the matter is. In the case U.2011.354Ø, the ship of the defendant was captured by Somalian pirates. The claimants, the employees of the ship, claimed that the captain had not established increased surveillance of the dangerous waters, and had not taught the crew to use the alarms designed for these situation. The judge agreed, but found the defendant to not be liable, even if they had acted carelessly, since the capture would have occurred regardless. If we apply this to our situation, it can be used by the defendant if they can prove, that the adversarial failures would have happened regardless of their careless behaviour. The analogy from pirates to adversaries is adequate, but yet again requires that the defendant reveals all details that could show, that the cyberattack was overwhelming enough to warrant them not being liable. We will return to this in section 3.4. But it is unlikely to succeed in court.

If the adversarial failure was caused inside the connected surgical robot, the link between carelessness and the injury is likely for the claimant to prove in court, because indirect proving would be possible, since a third party (the hospital) posses local data that can likely show the failure, or due to an indirect proof of it.

The last criterion is adequacy. Is it adequate that the link between the careless behaviour and the damage exists? This question is usually answered by case law, but this specific area has not been considered by the Danish courts. The claimant can argue, that because the defendant is a professional party, with objective liability and special role in both the product liability directive and the Medical Device Regulation, and because the harm is bodily, that the link is more adequate than not (Eyben and Isager 2013). The defendant would bring forth, that they should not be responsible for any kind of cyberattack directed at their produced machines, and that this should fall on the end user. But even if this is stated contractually, this does remove the fact they are the only party capable of effectively preventing some of the adversarial failures, which would lead to the judge most likely dismissing the last argument. The actions of third parties has been heavily discussed in the literature (Eyben and Isager 2013), and it is clear, that if a third party, such as the operator, caused the adversarial failure to occur by their actions, the defendant cannot be held liable. But situations where the action just made it more likely, does not mean that the defendant is off the hook. The defendant must prove this, easiest done with expert witnesses or compelling documentation, that could show for

example show why the cybersecurity or network security levels of the hospital were inadequate.

Nonetheless, it is likely that the link, if proven, is adequate nonetheless.

We see, that the patient can prove that the manufacturer acted carelessly, that an injury occurred, that a link between their injury and the carelessness, and it is likely that it is adequate. Unless the adversarial failure is subversion of robotic control, a lawsuit is likely to succeed.

3.3.2 Comments on Evidencing

Like before, the hardest parts of these lawsuits are proving the existence of the failure, and whether the manufacturer is responsible. Through case law, we know that the judges are willing to reverse the burden of proof, especially when they feel like they have a very low chance of uncovering the "hidden proof" (Eyben and Isager 2013). This refers to situations, where the actors that cause the damage are wholly owned and used by the other party, which the claimant here would have no way of proving anything about. This is also called presumption of responsibility, and it leads to a situation where, if the defendant cannot prove that they did not act carelessly, they will be considered liable (Eyben and Isager 2013). To reach this the claimant must encourage the idea in the mind of the judge, that the necessary documentation they need, will never come out of the defendant, unless they make use of this tool. But this tool is rarely used, and since we showed above that the case can most likely be decided without reversing the burden of proof, it is unlikely to be used. But the claimant should use it in the situation where the case would fail on proving the link, since the reversal would merely require the defendant failing to prove they did not act carelessly.

An example from case law would be U.2009.1652V, where an amusement park had to prove that their ride was correctly designed, instead of the injured party. They could not do so, which meant that they had to cover damages.

The courts can also choose to tighten the evaluation of carelessness, or assume responsibility to be objective because of the circumstances, with a central case for this being U.1957.109H. In it, a 14-year-old girl dropped out from an amusement park ride, and got injured. She did so because the back of the seat in the ride failed, and as she did not cause unusual strain to the seat, the supreme court concluded that the park was to cover her damages, since the seat was not strong enough for the task is was made for, and the park could not disprove this. While the judges at the time did not call it tightening of the evaluation of carelessness, it is later seen as such.

This can be used by a claimant to argue, that if the connected surgical robot and the infrastructure around it allow attacks that can cause bodily harm, they are not secure enough for their usage. But the distinction between what the manufacturer is expected to be able to defend against, which we considered earlier, is still apparent here. Like in the case where the manufacturer can only reinforce what they has control over, and nothing more. If this was to happen, it would allow the patient not to use resources to prove the first criterion.

3.4 Adversary specific aspects

Terrorist organizations, nation states, cybercriminals and organized criminal groups all require additional considerations.

If the adversarial failures are induced by parties who are covered by criminal legislation, here terrorists/cybercriminals and organized criminal groups, the cases would be different in practice. The police and prosecutors would collect evidence at first, which would make the burden of proof for both patient and manufacturer considerably lighter, since reimbursement and product liability cases can make of the evidence collected. Additionally, if organized criminals induced the failure(s), additional resources would be delegated to the investigation, and the potential punishments would be higher. Same goes for terrorists, since they are covered by anti-terror legislation.

Both they and nation states as adversaries can cause *force majeure*. This term in Danish law covers very unusual situations, where normal practice may not apply, which means the manufacturer is likely to not be kept liable. Stuxnet-like (Falliere, Murchu, and Chien 2011) malware can be a concrete example of sophisticated malware, that in practice would lead to situations where *force majeure* would be called by the defendant. The mentioned malware is an example of an attack that led to all our mentioned adversarial failures, at once, and similar overwhelming attacks from nation states cannot reasonably be expected to be defended against. This is what the defender of the manufacturer would argue. Acts of terror carry a similar connotation, and it would most likely lead to *force majeure* situations, unless the cyberattacks were simple and easily preventable.

But the adversary will matter, since a cybercriminal causing a failure is one thing, but a named terrorist organization causing it is completely different to a judge. The amount of resources available to prosecute organized criminal groups is higher as well, since they too have special legislation imposed upon them, which might lead to a lighter burden of proof for the patient.

4 The European Medical Device Regulation

In this section, we will introduce selected obligations and rights for manufacturers and regulators in the Medical Device Regulation[42]. We also relate them to the adversaries and adversarial failures, as well as some general cybersecurity considerations.

4.1 Background

The Medical Device Regulation is designed to achieve a balance between a high level protection of health for patients and users, as well as high standards for quality and safety of medical devices[43]. This fits the scope of the regulation,

---

[42]Regulation 2017/745.
[43]See preamble 2 in the regulation.

stated in art. 1(1), being a focus on laying down rules for placing medical devices on the market.
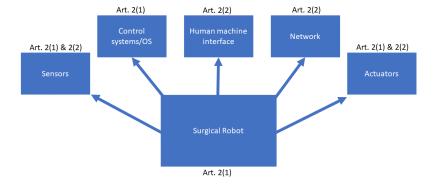
A regulation is a binding legal instrument, that is enforceable by the states and the EU, and usable (enforceable) by the relevant authorities as presented literally. This is derived from art. 288 in the TEU, which also defines directives as binding, but have them rely on the "form and methods" of the member states, with this generally meaning that the implementation is left to them instead.

It is natural to ask whether surgical robots are included within the regulation. We note that art. 1(1) includes any "medical devices for human use". This clearly encompasses connected surgical robots. Additionally, surgical robots are not included in art. 1(6), which constitutes the negative definitions (exclusions).

4.1.1 Accessories

Accessories of surgical robots will be governed by the same rules as the robots they are used with, see art. 1(1). However, we must define what accessories are in this context as stated in art. 2(2). Any traditional accessory that is also a medical device, such as respirators that could be used during operation, are covered in art. 2(2) first part. But the second part expands and includes anything that is "to specifically and directly assist in the medical functionality of the medical device(s)". To be considered an accessory, it must specifically and directly assist with the medical functionality of the surgical robot, for telerobotic surgery this is both the encrypted connection, the local network that enables it and the operator screen and equipment that controls it elsewhere.

Figure 3: Example of accessories of a surgical robot.

This does not mean that the accessories, if not directly a part of the connected surgical robot, are under the responsibility of the manufacturer. The operator or end user must maintain and keep them updated, and a separate evaluation on whether they would be considered medical devices is taken by the member state, see preamble 8 in the regulation. The regulator that decides resides in the place of business of the accessory manufacturer. But if the accessories, such as specific equipment for the physical part of the surgery, are a direct part of the robot, the manufacturer is responsibility for any safety or security issues they present.

4.1.2 Entry into force

As of the time of writing, the application of the Medical Device Regulation has been postponed[44]. Despite this, we have decided to use it instead of the existing medical device directive, since that will be obsolete by 26/05/2021.

4.2 Guidance on Cybersecurity

Like national law, EU-law has additional documentation and guidance that can be used by different parties affected by it. One of these the is guidance on cybersecurity for medical devices, which is made by the Medical Device Coordination Group (MDCG)[45]. Guidance can be seen as legally binding[46], a tool to guide interpretation or at least act as guidelines for the parties. We make use of it for interpretation specifically.

The MDCG, while having created this, does not make legally binding guidance, as there is nothing stating this in the regulation, but in the future art. 103(8) does allow them to create recommendations or opinions in emergencies. For this reason, we have to view the guidance on cybersecurity as soft law[47].

While the regulation does not explicitly consider the safety to security problems, the guidance does on page 10. It equates security risks having a safety impact, which here for us would refer to damage to a patient caused by an adversarial failure. It argues that because of this, Annex I has to both be interpreted in a safety as well as a security manner.

4.3 Manufacturers

Surgical robots can be put on the market by several different parties, and as mentioned earlier, we have chosen the manufacturer as the most important one, due to their central role in the robot's life cycle. As a general rule, the manufacturer answers only to the regulator in its place of business, see art. 10(14). However, any patient in any member state can sue any manufacturer, because

---

[44]Described in Regulation 2020/561, which was created to give affected national regulators time and resources to respond to the Covid-19 crisis.

[45]Established by art. 103 in this regulation.

[46]This is prevalent in national law, if the guidance is purely made for a specific public authority, but can be problematic to always impose in EU-law.

[47]A legal source that is not binding, but can affect how other sources are interpreted.

of the rule of special jurisdiction from art. 7 in regulation 1215/2012[48].

We have selected several obligations [49] which are:

1. The system of risk management, art. 10(2).

2. The system for quality management, 10(9).

3. Sole responsibility for devices, 10(1)(12)(13)(14).

4. A system for financial responsibility, 10(16).

5. Annex I specific obligations.

The system of risk management. This is defined in Annex I, section 3. It is a continuous iterative process through the surgical robot's entire life cycle. The system has to identify and analyse all foreseeable hazards, estimate and evaluate risks associated with/occurring during intended use and the future, eliminate or control those and evaluate this information and combine it with the data gathered from the post-market surveillance system[50].

The term hazard does not literally include adversarial failures, but since they can cause hazards in a safety manner, like the surgical robot jumping or possible getting hijacked which risks the patient and anyone nearby, they should naturally be included. Theft of trade-secrets or software vulnerabilities cannot directly cause physical harm, and should therefore not be included. But from this, all other adversarial failures must be eliminated or controlled. The guidance summarizes these parts of the system as a circular information flow, consisting of a risk management plan, assessment, risk control, evaluation, review(s) before release and post-market activities, see p. 17. But this is not directly derived from the regulation.

The system of quality management. While this system includes the risk management above, it also has others elements that are relevant to us. Firstly, identification of applicable general safety and performance requirements/exploration of options to address it. This is mandated, and must be addressed separately from the rest. Secondly, the post-market surveillance system, which in cybersecurity terms must catch all incidents moving forward.

Sole responsibility. The term sole responsibility refers to the manufacturer's role as both the creator, controller in art. 10(12) in the sense that any non-compliance on the device has to be relayed to the regulator, and as a partner with the regulator, since they have to cooperate and follow requests given in

---

[48]Regulation on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters.

[49]We omit clinical evaluations/investigations.

[50]As seen in art. 83, which requires manufacturers to have a system in place for surveillance of the post-market situation of their device, be it academic or technical data.

art. 10(14). This flips back to art. 10(1), which solely states that the devices should be designed and manufactured to comply with the regulation. Generic software, other than it being being updated, is not included, as is accessories that are also medical devices. But other accessories are.

A system for financial responsibility. This is defined in art. 10(16), where compensation schemes specific to each country are mentioned, which usually involves initial insurance coverage, but also product liability lawsuits and national law. The risk class, type and size of the manufacturer plays a role in which measures, like insurance, that they have to undertake, but the article takes national protective measures into account – this includes Patient Reimbursement from earlier. This shows that the regulation leaves all legal remedies and considerations concerning litigation up to the member states and insurance solutions.

Annex I. By itself, this annex further defines requirements for the medical devices, and according to the guidance and if read literally, section 17 on electronic programmable systems should be the focus when it comes to connected surgical robots. Section 17.1 requires that the devices are designed for repeatability, reliability and performance. If a single "fault" is found, it has to be eliminated or reduced as much as possible. Whether fault only refers to non-adversarial failures or the opposite is unclear, but considering the guidance's emphasis on this part, an interpretation that sees it as adversarial failures is appropriate. This is supported by safety faults being the focus elsewhere. Since these requirements are not part of the risk management system, this further emphasizes that any adversarial failure that can affect the three terms above must be prevented, which means that the failure of theft of trade-secrets is likely to not be considered.

Section 17.2 requires the software used in devices to be developed/manufactured with "state of the art". State of the art is used sparingly in the regulation, but has not been included in any of the central articles. The term equates to regular updates and maintenance of the software, and it has to consider the life cycle of the device and information security, verification and validation of it. The three last categories would imply that it should catch all adversarial failures, with security preventing manipulation attacks and subversion of robotic control and perhaps theft of trade-secrets, verification catching reprogramming of the robot and poisoning of the feedback loop, and validation[51] reinforcing whether the security is adequate or not. State of the art would then prevent software vulnerabilities by regularly identifying and erasing them. However, state of the art only requires what term encompasses, which also means that anything that the industry does not know or what is not expected of it, it does not require the manufacturer to do. This includes which adversaries that should be defended against, with nation states being impossible to include because of their immense power.

---

[51]Refers to testing of cybersecurity.

Section 17.4 requires that the manufacturers decide on minimum requirements for hardware/IT networks characteristics/IT security measures, that allows the software to run as intended. This allows the manufacturer to technically set standards that could be problematic in the long run, since it might not prevent more complicated and dangerous developments.

Now we move on to the rights of regulators, and how that plays into the cybersecurity of connected surgical robots.

4.4 Regulators

The other subject, the regulator, is defined as the competent authority, which the member states designate themselves, see art. 101. We select several rights from the regulation which are:

1. Right to request documentation and punish the manufacturer if they do not cooperate, art. 10(14).

2. Market surveillance activities, art. 93.

3. Evaluation of devices suspected of presenting an unacceptable risk or other non-compliance, art. 94

4. Procedure for dealing with devices presenting an unacceptable risk to health and safety, art. 95.

5. Other non-compliance, art. 97.

Art. 10(14).   This part of the article contains the special right for the patient in its paragraph 3, but we focus on 1 and 2. In paragraph 1, the manufacturer must provide documentation to demonstrate conformity of the device, or samples free of charge or access to the device. Further, they have to cooperate on any corrective action to eliminate or reduce risk for devices they put on the market.

If this is in some way not possible, the regulator has the right in paragraph 2, to take all appropriate measures to prohibit/restrict/withdraw/recall the device, see art. 10(14) second paragraph. The right is not built up as an immediate use of force, but rather the opposite. It is instead based on trust in the manufacturer fulfilling the requests from the regulator dutifully. It is not specified whether the regulator has the necessary knowledge or personnel, to request actions or documentation that relates to cybersecurity, but because of the existence of the guidance this might be the intention.

Market surveillance activities.   This activity resembles what most are familiar with from national food regulation authorities. Review of documentation, physical or laboratory checks are possible, as is requesting documentation from other parties than the manufacturers and unannounced inspections. How this can be applied to cybersecurity cannot be literally read, but considering the

wide power the regulator has it is theoretically able to thoroughly review and inspect risks that might lead to adversarial failures.

Art. 94. If the regulator takes notice of there being an unacceptable risk to the health/safety of patients/others, or if the device seems to not comply in general, they then carry out a more thorough investigation that includes the complete check of compliance of the regulation. Whether this includes penetration testing or other validation measures of the devices would be intriguing, but the possibilities exist if the threat of cyberattacks increase, or if post-market surveillance has shown specific issues.

Art. 95. If the regulators are confirmed in their suspicions, they first ask the manufacturer to take all appropriate and duly justified corrective actions to restore compliance, and until then, themselves proportionally restrict the availability of the device. The latter means recalling the device in practice. And if this is not done, this loops back to art. 10(14), where the regulators can forcefully remove the robot from the market.

Art. 97. If the evaluation showed other non-compliance, the regulator can react in a similar fashion. The requirement for unacceptable risk to health etc., is not present here, but the powers are the same. This is interesting, because this can potentially include adversarial failures that do not have a risk to the health and safety of anyone, for example theft of trade-secrets and software vulnerabilities. It remains to be seen how this can be used in regards to connected surgical robots.

4.5 Discussion of the regulation

It is no secret, that the Medical Device Regulation does not literally mention cybersecurity, adversarial failures or even robots. This is because it is a EU regulation, which strives to encompass all possible medical devices, seen in art. 1(1). We do not criticize or comment on this, but it is also the legal framework for connected surgical robots for the foreseeable future. No one would doubt that the regulation improves and continues what the directive did[52]. But we have to discuss the specific findings, negative and positive, that we have found.

The regulation chooses to not have a focus on utmost prevention of adversarial failures *ex ante* [53], and explicitly does not say this outside of the annex and vaguely in other spots. If it had done this, both the safety and security of the patient would have been the focus. However, the safety of the patient is not mentioned in art. 1, which shows that it is not the scope of the regulation. This does not mean that issues cannot be addressed in practice by the manufacturers and regulators, and preamble 101 leaves room for further legislation down the line, to ensure the goals of the regulation, which could include rules

---

[52]See preamble 4.

[53]Issues solved before.

for cybersecurity specifically. Future case law at ECJ can also further address these issues.

The choice of leaving many important cybersecurity issues to a guidance is likely deliberate. But the future of healthcare is in the field of CPS, which will have issues with adversarial failures. The decision to equate safety issues with security issues because of cybersecurity, in a guidance instead of the regulation is not adequate considering the guidance is not legally binding. But as shown, the guidance functions well as a tool to interpret articles and the annex. And it is possible that there will be *lex specialis* that manages the specific issues that the field presents later, but they are unlikely to initially be regulations, and will therefore have less weight in the world of EU-law.

4.5.1 In regards to manufacturers

Even with quality and risk management systems, defined rights for regulators and tight obligations for manufacturers, and a forced state of the art idea in place, one must doubt if the manufacturers would still prefer to let the accidents happen, and let litigation solve any issues later. Prevention is mentioned in the regulation, but if it fails to enforce prevention in specific technical, yet physically dangerous aspects, such as those CPS represent when adversarial failures occur, it ends up having to solve these issues as they happen.

However, the regulation does succeed in stating separate obligations to reinforce cybersecurity, with the same systems and the requirements in Annex I cumulatively functioning together.

4.5.2 In regards to regulators

As can be seen, regulators do not have to explicitly fulfil any cybersecurity obligations[54], but the question remains whether they can each sufficiently inspect and regulate the cybersecurity of connected surgical robots. There is not a literal requirement for this in the regulation. Art. 101 merely defines how that the regulator has to be designated, but there is nothing concerning specific specialized staff that can handle cybersecurity. This is widely different compared to regulations such as the GDPR[55] which lays down a rigorous structure. Instead, the MDCG are supposed to coordinate efforts across the EU, but they are not specified enough to inspect or enforce practice in art. 103.

It is clear that the regulators rely on documentation and information gathered by the manufacturers and its partners, as seen in clinical evaluations and investigations[56] which we have not covered, but as shown they also posses several rights that in the future could be central. Inspections, requests to correct issues and the sharing of all documentation between all regulators from all possible manufacturers via the MDCG and their systems, as well as forcefully moving dangerous medical devices off the market by any means, show that the system

---

[54]Outside of maintaining and being part of the various information sharing systems.
[55]General Data Protection Regulation, 2016/679.
[56]See Chapter VI in the regulation.

and its players may solve some of the issues we have shown with the regulation. This includes the special right for patients in art. 10(14), mentioned earlier, that enables them to make use of the documentation gathered by the regulators as well.

5   The NIS Directive

Operators and users of surgical robots, be it private or public hospitals, have to fulfill the requirements set out in this directive. This is because they are considered operators of essential services, as they fulfill art. 5(2) in the directive. Their service is essential for critical societal activities, make use of network and information systems, and an incident would have significant disruptive effects on the provision of that service. The last requirement is seen where patient data is not available, equipment like surgical robots that rely on access to a network loosing it, and most importantly, adversarial failures on equipment. They are further seen as operator of essential services in Annex I, 6. Because of this, states decide on appropriate and proportional technical measures to prevent risks, incidents and notification of incidents to authorities in art. 14.

In a Danish context, all hospitals report directly to the Danish Financial Supervisory Authority and Center for Cybersecurity.

But this does not concern the manufacturers of surgical robots. At most, due to their provision of maintenance of the robot, they are considered digital service providers. But like essential service providers, manufacturers would have to fulfill similar obligations as those in art. 14, but from art. 16 instead. But only from where the manufacturer has its place of business, see art. 18. In a Danish context this would imply, that only Danish produced surgical robots would come under Danish jurisdiction.

This shows, that there was no reason to include considerations from the NIS directive in this paper, since they would not apply directly as the manufacturers of most surgical robots are not currently placed in Denmark.

But the NIS directive is mentioned and emphasized by the guidance on cybersecurity attached to the Medical Device Regulation, but since its implementation is done on a country to country basis, listening the approach to the directive for every member state is outside the scope of this paper.

6   International Perspectives

Since the types of cyberattack that can hit surgical robots and CPS will be the same in every jurisdiction, any considerations about possible legal remedies is relevant. And while most principles from our used law cannot be applied elsewhere, the ideas behind them should be considered. Exporting the new rules from the regulation is currently not wise, as it has not been tried in practice. However, what was shown in Danish law is tried and true.

Letting an injured patient or their family choose between traditional litigation in courts, which has high initial costs, and an administrative system that is free, and potentially can recover the same exact amount of damages as one would get in court, should be interesting to other countries. Especially when it is able to embrace new technology by disregarding it, and dismiss the safety and security differences, and only focus on the fact that the connected surgical robot failed during operation. But, it is required that there exists public law in the background, that forces the authority to conduct a full and proper investigation, even if the patient is unable to prove anything. If such a system is in place, and it always stands by what we have shown, it will always catch all patients that might get injured due to adversarial failures in the future.

We could express this as three principles:

1. If a surgical robot fails, for any reason other than the patient themselves causing it, the patient shall have their damages fairly covered.

2. Regardless of whether the healthcare provider or third party caused the injury, the liability always rests on the healthcare system at large.

3. Compensation can only occur, if the surgical robot is directly or indirectly used by a national healthcare system, where the system, whether state run, fully privatized or anything in between, pays to a compensation scheme without question.

They expresses the rules fully, and include an evaluation of fairness, as well as requiring them to be part of a national system, so that the state can compensate initially. It does have a central weakness, which is common in administrative systems, since its practice can change based on the decisions it makes. Indeed, this makes the system highly flexible, but at the risk of changing the interpretation to not see cyberattacks as failures.

Even if the healthcare system was to be partially or fully privatized, as long as this administrative system was still in place, and all hospitals dutifully provided all documentation and were parties in a comprehensive insurance system, the idea of full compensation presented would still be possible. This is because the principles implicitly require full enforcement and cooperation, but if these lack, it is not possible to run in practice.

The principles have room for a different system of contracts/tort or reimbursement idea in the idea of "fairly". Systems with objective or looser liability for healthcare providers, will not have issues since the liability is always assumed. This is stated in principle 2.

7   Future and Related Work

In this section, we look at important related work and future work that is necessary to due because of this paper.

7.1 Related Work

There is a limited amount of work surrounding liability and surgical robotics. Beglinger, Christopher has written a note (Beglinger 2020), which explores non-adversarial failures and liability for surgical robots in an American perspective. It draws many useful insights from the legal sphere of product liability, as well as showing the holes that get created specially with accidents involving these devices. It further showed that there exists room for national analysis in academia considering surgical robots, whether connected or not.

Holder, Chris et al. (Holder, Khurana, Harrison, et al. 2016) (Holder, Khurana, Hook, et al. 2016) have in their two part series on robots and legal implications also addressed surgical robots. They serve as the best introduction of what we have discussed from a high level, as well as an introduction to surgical robotics as such.

7.2 Future work

In the future, if adversarial failures become commonplace, this might lead to it not being considered a defect or a failure in the Patient Reimbursement system. Considerations on this topic outside or inside of the CPS sphere or as interdisciplinary work is highly needed, since more infrastructure rely on it.

Analysis on when a cyberattack constitutes a defect in different bodies of EU memberstates' law is necessary as well, since it is not clear whether the product liability directive answers this. A general discussion of cybersecurity and defects on an international level is needed too.

Another area that needs further work is the Medical Device Regulation in general. Even if it itself declares that it has not changed significantly since its directive form in preamble 4, but rather been reinforced, this does not mean that it will not be applied differently in practice. Wording means everything in EU-law, and the clearer we are on what it means, the better, inside as well as outside cybersecurity related issues. Like we touched upon earlier, research into what constitutes accessories to medical devices is necessary, as well as which responsibilities the manufactures of the accessories have, even considering future guidelines or case law.

8 Concluding Remarks

Having surgical robots connected to the internet seems like a nightmare come true. Adversaries now have access to the very instruments that save lives, and can potentially manipulate or at least disturb the surgery. In this paper, we found that legal remedies do exist in Danish law, if one was injured because of a cyberattack on a connected surgical robot. The remedies are either lawsuits or an administrative procedure.

First, we find that the issue of proving anything in court can be a major obstacle for both types of lawsuits. Design documentation, log files and other documentation that the manufacturer has access to, is not initially able to the

patient. But because civil lawsuits rely on free argumentation from both parties, the patient can indirectly force such proof out, or from 2021 with the help of the regulator via the Medical Device Regulation art. 10(14). This is show in Danish case law in both types of lawsuits to be possible, even if it came from safety instead of security practice.

We found a lawsuit based on product liability possible, if it was based on the EU directive or case law based approach in Danish law, but not if it was based on contract. It requires that the surgical robot is put into circulation, so completely custom made versions are exempted. Especially the use of *res ipse loquitur*, which is showing that nothing else but an adversarial failure or a cyberattack could have caused it would indirectly show that the defect exists. This, supported by case law, would show the link between the defect and the injury, but the defendant has one last defense they can ask for which is the case law based test of "systemic damage". If the danger cyberattacks pose are known, and unavoidable, the defect is not considered to be so. But both questions have to be answered with a no in most situations, because the risk of cyberattacks are not know by the public for the product, and only subversion of robotic control as a cyberattack can be considered unavoidable. Therefore, the defendant is unlikely to be able to use the test.

We showed that the patient is able to sue for damages via reimbursement outside of contract, but proving the link between the attack and the injury is difficult. Indeed, if the cyberattack was subversion of robotic control, which involves factors outside CPS, the link is likely impossible to prove. And the patient can further attempt to argue, that the needed knowledge is kept so closely to the other party, that it would be better shown if the judge reverses the burden of proof, which would bypass all needs to prove any criteria necessary to use this approach, and instead force the manufacturer to prove that the surgical robot is designed appropriately. Else, we found that the rest of the criteria required for this approach are likely to be true, which means that this approach is possible to proceed with in court.

And finally, the most secure way to cover damages, is to make use of the Patient Reimbursement system. Instead of suing the manufacturer of the robot that was attacked, the patient can choose to submit a free application to the Danish Patient Reimbursement Authority, and get their damages fully covered[57]. This is only between the state and the patient. It is sure to succeed, because the rules surrounding this dictate, that if the machine fails, no matter the cause, the patient is entitled to have all their damages fairly covered.

This shows, that while cybersecurity and cyberattacks have not been explicitly considered in any of the legislation or case law, they can still fit the existing legal framework.

We can illustrate which remedies were possible and which were not:

---

[57]If they were deemed to have been injured.

Law	Product Liability	Patient Reimbursement	Reimbursement in court
Unlikely	0	0	0
Likely	X	X	X
Highly likely	0	X	0

On a more negative note, we showed that the European Medical Device Regulation that governs surgical robots does not consider cybersecurity aspects, if one reads it literally. There are considerations about the health and safety of patients, but not specifically about the risk that cyberattacks pose. Only the guidance that comes with the regulation, as well as a expanded interpretation on its rules of the risk and quality management come close to outright requiring a focus on security. This is the classical example of a broad piece of legislation, with all the issues that come with it.

But, like other EU-law, there is a possibility that the Union can take subsidiary measures to fill out what the regulation misses[58]. We interpret several requirements as including cybersecurity, and since several state elimination of risks and security levels, they have a higher chance to work in a cumulative manner. One set of requirements can have its issues, but when it is stated in both articles and in Annex I, this increases the chance of it having a discernible effect. Furthermore, there is the possibility of future legislation down the line, as well as a wide toolbox for the regulators to inspect, withdraw and generally keep a close eye upon the connected surgical robots if they are willing to do so. The latter has yet to be seen, and while useful, there is no guarantee that the regulators have the staff or finances for it.

We argue, that manufacturers of surgical robots are, at most, considered digital service providers in regards to the NIS directive, and that it has no impact on our analysis as such.

In terms of lessons for other systems, we argue that the model seen in the Patient Reimbursement system is the most appropriate to deal with the issues cyberattacks on connected surgical robots presently, as long as there exists public law in the background that assure proper proving and procedure, and that the parties, whether private or state run, always fund the compensation scheme and provide documentation.

---

[58]See preamble 101.

References

[AKS96]   Taimur Aslam, Ivan Krsul, and Eugene H. Spafford. "Use of A Taxonomy of Security Faults". In: *Proceedings of the 19th National Information Systems Security Conference* (1996), pp. 551–560.

[AL10]   Mads Bryde Andersen and Joseph Lookofsky. *Lærebog i obligationsret.* 4th. Vol. 1. Karnov Group, 2010.

[Al94]   CARL E. LANDWEHR et. Al. "A Taxonomy of Computer Program Security Flaws". In: *ACM Computing Surveys* 26.3 (1994), pp. 211–251.

[Ale+16a] Homa Alemzadeh, Daniel Chen, et al. "Targeted attacks on teleoperated surgical robots: Dynamic model-based detection and mitigation". In: *Proceedings - 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2016* 395 (2016), pp. 395–406. DOI: 10.1109/DSN.2016.43.

[Ale+16b] Homa Alemzadeh, Jaishankar Raman, et al. "Adverse events in robotic surgery: A retrospective study of 14 years of fda data". In: *PLoS ONE* 11.4 (2016), pp. 1–20. ISSN: 19326203. DOI: 10.1371/journal.pone.0151470.

[Bar+12] Michael J. Barry et al. "Adverse effects of robotic-assisted laparoscopic versus open retropubic radical prostatectomy among a nationwide random sample of medicare-age men". In: *Journal of Clinical Oncology* 30.5 (2012), pp. 513–518. ISSN: 0732183X. DOI: 10.1200/JCO.2011.36.8621.

[Beg20]   Christopher Beglinger. "Note A Broken Theory : The Malfunction Theory of Strict Products Liability and the Need for a New Doctrine in the Field of Surgical Robotics". In: (2020), pp. 1041–1094.

[Bon+15] Tamara Bonaci et al. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots". In: (2015), pp. 1–11. arXiv: 1504.04339. URL: http://arxiv.org/abs/1504.04339.

[BY14]   Christos Bergeles and Guang Zhong Yang. "From passive tool holders to microsurgeons: Safer, smaller, smarter surgical robots". In: *IEEE Transactions on Biomedical Engineering* 61.5 (2014), pp. 1565–1576. ISSN: 15582531. DOI: 10.1109/TBME.2013.2293815.

[Car09]   Alvaro A. et al. Cardenas. "Challenges for Securing Cyber physical Systems". In: *Computer Audit Update* 2009.3 (2009), pp. 3–6. ISSN: 09602593. DOI: 10.1016/0960-2593(92)90002-5.

[EI13]   Bo von Eyben and Helle Isager. *Lærebog i erstatningsret.* 7th. Jurist- og økonomforbundets Forlag, 2013.

[FMC11]   Nicolas Falliere, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier". In: *Symantec Security Response* 14.February (2011), pp. 1–69. URL: `http://large.stanford.edu/courses/2011/ph241/grayson2/docs/w32%7B%5C_%7Dstuxnet%7B%5C_%7Ddossier.pdf`.

[GGØ15]   Bernhard Gomard, Hans Viggo Godsk Pedersen, and Anders Ørgaard. *Almindelig kontraktsret*. 4th. Jurist- og økonomforbundets Forlag, 2015.

[Hoc+07]   N. G. Hockstein et al. "A history of robots: From science fiction to surgical robotics". In: *Journal of Robotic Surgery* 1.2 (2007), pp. 113–118. ISSN: 18632483. DOI: `10.1007/s11701-007-0021-2`.

[Hol+16a] Chris Holder, Vikram Khurana, Faye Harrison, et al. "Robotics and law: Key legal and regulatory implications of the robotics age (Part i of II)". In: *Computer Law and Security Review* 32.3 (2016), pp. 383–402. ISSN: 02673649. DOI: `10.1016/j.clsr.2016.03.001`. URL: `http://dx.doi.org/10.1016/j.clsr.2016.03.001`.

[Hol+16b] Chris Holder, Vikram Khurana, Joanna Hook, et al. "Robotics and law: Key legal and regulatory implications of the robotics age (part II of II)". In: *Computer Law and Security Review* 32.4 (2016), pp. 557–576. ISSN: 02673649. DOI: `10.1016/j.clsr.2016.05.011`. URL: `http://dx.doi.org/10.1016/j.clsr.2016.05.011`.

[Kob16]   Kazukuni Kobara. "Cyber physical security for Industrial Control Systems and IoT". In: *IEICE Transactions on Information and Systems* E99D.4 (2016), pp. 787–795. ISSN: 17451361. DOI: `10.1587/transinf.2015ICI0001`.

[NPH08]   Günter Niemeyer, Carsten Preusche, and Gerd Hirzinger. "Telerobotics". In: *Springer Handbook of Robotics*. 2008. Chap. 31. Pp. 741–757.

[NSF14]   NSF. *Cyber-Physical Systems PROGRAM SOLICITATION NSF 20-563*. Tech. rep. 2014, pp. 1–20.

[PMB15]   Dorottya Papp, Zhendong Ma, and Levente Buttyan. "Embedded systems security: Threats, vulnerabilities, and attack taxonomy". In: *2015 13th Annual Conference on Privacy, Security and Trust, PST 2015* (2015), pp. 145–152. DOI: `10.1109/PST.2015.7232966`.

[Qua+17]   Davide Quarta et al. "An Experimental Security Analysis of an Industrial Robot Controller". In: *Proceedings - IEEE Symposium on Security and Privacy* (2017), pp. 268–285. ISSN: 10816011. DOI: `10.1109/SP.2017.20`.

[Riz+18]   Syed Rizvi et al. "Securing the Internet of Things (IoT): A Security Taxonomy for IoT". In: *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* (2018), pp. 163–168. DOI: 10.1109/TrustCom/BigDataSE.2018.00034.

[VB13]   Milos Vasic and Aude Billard. "Safety Issues in Human-Robot Interactions". In: *2013 IEEE International Conference on Robotics and Automation* (2013).