Everything-as-a-Hack: Claims-Making for Access to Digital and Social Resources

Wolter Pieters
TU Delft
Delft, Netherlands
w.pieters@tudelft.nl

ABSTRACT

In media and public discourse, cyber incidents are typically covered in terms of cybercriminals or other external threat agents managing to gain access to sensitive data and systems through weaknesses in technology and/or human factors. Such a framing of incidents foregrounds the (problematic) access claims of "hackers" and the protection against those as the key issue in security. However, other access claims play a role in the same incidents, such as those of the data owners, service providers, advertising companies, intelligence agencies, etc. These access claims are made via different means, and they are backgrounded when the problem is framed in terms of unauthorised access through hacks. In this contribution, I investigate the activity of *claiming access* as a key analytical concept in a more symmetrical treatment of cybersecurity and associated incidents. Rather than implicit, normalised, and technologically congealed notions of threats and associated access claims, this analytical framework aims at highlighting *all* access claims within the scope of a cybersecurity phenomenon, in order to uncover the politics behind cybersecurity and associated discourses and infrastructures, and thereby increase transparency. By covering different types of resources and different means of access, the approach also has the potential to connect the rather separated discourses on cybersecurity, privacy, and social manipulation through technology.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; *Economics of security and privacy*.

ACM Reference Format:
Wolter Pieters. 2019. Everything-as-a-Hack: Claims-Making for Access to Digital and Social Resources. In *New Security Paradigms Workshop (NSPW '19), September 23–26, 2019, San Carlos, Costa Rica.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3368860.3368868

1 INTRODUCTION

Cybersecurity incidents and associated harm receive more and more attention in media and public discourse. In most cases covered, cybercriminals or other external threat agents manage to gain access to sensitive data and systems through weaknesses in technology and/or human factors. Thus, cybersecurity issues are framed in terms of problems with "hackers" obtaining unauthorised access. Currently, a specific worry is related to the so-called Internet-of-Things: with cameras, washing machines and children's toys connected to the Internet, what additional harm can those hackers do? At the same time, we give the data associated with these devices away to the service providers without much consideration, such as what we watch on our digital TV. The use of that data in ways that may harm us is typically considered in terms of privacy, not security. But aren't the two threats very similar in the sense that access is being claimed to some resource by some agent, albeit through different means?

This begs the question how access claims, both by hackers and others, function in the discourse on cybersecurity. Instead of foregrounding the means of access, typically highlighted in cyberattacks through specific actors and specific attack vectors or technical vulnerabilities, this approach foregrounds the underlying (political) claim, the activity of claiming, and its impact on the resulting access relations. This means that service providers obtaining access to data through providing a service will be treated in the same fashion as hackers obtaining access through exploiting software vulnerabilities. This paper therefore proposes an approach focused on access claims to analyse the dynamics of stakeholders and resources in cyberspace. This approach enhances transparency of the political processes underlying cybersecurity discourses, and contributes to a symmetrical and inclusive (i.e. non-excluding) understanding of access relations and associated threats. It also provides possibilities to connect the rather separated discourses on cybersecurity, privacy, and social manipulation through technology, as all these phenomena involve underlying access claims. The central hypothesis is that the notion of access claims provides a more general lens to study such phenomena than focusing on specific threats and specific means of access.

First, we will take a look at how entities and means of access are currently foregrounded as security threats, and how such threat models become normalised, thereby hiding other access claims. Second, access, claims, and the combined concept of access claims are discussed, to establish a conceptual framework that can open up the black box of current threat models. Third, operationalising this framework for the digital domain is done in dialogue with approaches focused on political claims-making as well as literature on access claims and associated claims-making processes for natural resources. Fourth, the different stages in the lifecycle of access claims are discussed. After establishing these components of the analytical framework, I sum up the key analytical contributions, and apply them in two cases: Internet-of-Things (IoT) and fake news. I conclude that analysing cybersecurity phenomena in terms

NSPW '19, September 23–26, 2019, San Carlos, Costa Rica

ACM ISBN 978-1-4503-7647-1/19/09…$15.00
https://doi.org/10.1145/3368860.3368868

of access claims and claims-making processes can broaden the discussion beyond normalised threat models, and thereby enhance transparency of the underlying strategies and politics.

2 SECURITY AND THE BAD GUYS

Security threats are typically defined in relation to some system in which they could intentionally cause harm. As harm is defined in relation to stakeholder goals, who is considered a security threat depends on the stakeholder perspective taken. In this respect, what is considered creative use by some may be considered misuse by others [33].

Hackers are in this respect an example of "creative users". In fact, hackerspaces and similar initiatives emphasise precisely this aspect. To distinguish hackers from computer criminals, the latter have sometimes been termed "crackers" [1, 36]. The framing is important here: relabelling oneself in terms of security status may be decisive in terms of whether one is seen as a creative user or as a misuser / security threat.

In a supposedly common sense view, cyber threats originate from figures such as crackers who attempt to break into a computer system from the outside, using either advanced technical means or manipulation tricks. Hackers, crackers, cybercriminals, etc. all point towards external sources, suggesting that maintaining boundaries with the ruthless outside world is a good idea. Quite some work in the security space has already emphasised that security threats do not only come from outsiders, nuancing the naive fortress view. In fact, "insider threat" has become part of the standard information security vocabulary [4, 27, 30]. Nevertheless, this broadening of the threat portfolio refers primarily to (disgruntled) employees that threaten an organisation from within, rather than generalising the threat concept to any kind of access relation. Even the concept of "external insider" [11], including actors such as subcontractors, still sets limits on who can be considered a threat.

What we currently see is that hackers are only a (small?) subset of those that use technology in creative ways in order to obtain access. Especially under the umbrella of what critics call "surveillance capitalism" [40], large amounts of (personal) data are harvested through the provision of services, such as in social media. The notion of "dark patterns" corresponds to "hacks" in which people are persuaded to share personal information [5, 14]. In fact, this strongly resembles traditional forms of "hacking" through social engineering, in terms of the persuasive techniques being used, although both terms seem to be rather disconnected in literature.[1] All these developments involve claims to access.

In addition, problematic access does not need to be confined to (digital) data. Dark patterns may aim at data, but also simply at keeping the user's attention, which is scarce in the attention economy. Platforms such as booking.com and Amazon monopolise access to sellers and buyers [34]. Current discourses on fake news and other forms of social manipulation through technology question the ability to influence people's opinions. These phenomena seem to be focused on problematic access to *social resources*, albeit via digital means. They also point to different types of agents that may claim problematic access to resources via different channels.

[1] In fact, one of the few papers mentioning both terms is [3], which also tries to connect different phenomena, in this case under the umbrella of misinformation.

Also in the Internet-of-Things, it is not only access claims of hackers that play a role. Many access claims in the Internet-of-Things are due to a transition from things to services. Whereas producers used to have no business in how we used our devices, this is changing with the current generation of devices that "phones home", informs the provider about our behaviour, and enables the provider to change functionality. Again, this access claim is fundamentally not very different from a hacker claiming access to a system, although the strategy to enforce the claim is different.

Platforms, social media and IoT involve access claims in the commercial domain. At the same time, countries are debating how much access the police and intelligence agencies should be able to claim, and what the role of service providers is in granting such access. Both in formal (government) surveillance and in commercial forms of surveillance, access claims play a key role. In addition, depending on the stakeholder perspective, such access claims may be seen as threatening.

As we saw in the case of social engineering (a form of hacking) and dark patterns (generally not considered a form of hacking), there is a gap between what is included in security threat models, and what is excluded, or at least not discussed in the same terms. It seems that we have learnt to look at threats in terms of certain categories [25], which do not cover the entire spectrum of similar phenomena. This is partly a natural process of sense-making in complex environments, and it points to the intricacies of the social construction of reality [2]. However, there is also a component of strategic framing here, allowing stakeholders to represent security and privacy problems by categorising threat actors in such a way that they themselves are excluded. For example, social media services may frame privacy in terms of inter-user access, with lots of associated settings, hiding the issues of user-provider privacy.

Overall, the conclusion should be that there are implicit and normalised threat models in play in the key developments affecting cybersecurity. That is, the decision on which stakeholders are labelled as threats and why is not subject to scrutiny, excluding other stakeholders from being considered as being involved in access-claiming activities. Such hiding may be both unintentional (we simply don't see the full picture because of the complexity and the setup of the existing discourse) or intentional (stakeholders strategically frame security issues in terms of access by others). Based on such framing, patterns of access can emerge that withhold access from some stakeholders, while granting potentially equally problematic access to others. The access may be explicitly legitimised via political decisions, but it may also have gradually developed and become accepted without explicit legitimisation.

We thus see that in security and associated debates, implicit and normalised threat models hide the complexity of the situation. In different contexts, the idea of problematic access has evolved to carry different associations, with particular types of problematic access being foregrounded, blurring the connection to similar phenomena. This begs the question whether a richer conceptual framework could be devised to analyse security, both in settings of controversy and in stable ones. In this paper, I hypothesise that the notion of access claims and the associated activity of claiming access can serve as the basis for such a framework.

3 ACCESS, CLAIMS, AND SECURITY

In order to understand the role of access claims in security, let's first have a look at the definitions of the composing terms. First, there is the notion of claim.

Claims can mean different things in the context of security, and the concept is connected to the concept of security arguments. Security arguments, as opposed to claims, have been discussed before [17, 26], in particular in terms of justifying assessments of security risk and selection of security controls. The main difference with this line of research is that I do not focus on knowledge claims here ("an assertion that something is true"), but on entitlement claims ("a demand or request for something considered one's due").[2] Thus, claims in this paper refer to a demand or request for access rather than statements about (the effectiveness of) security controls. Similarly, this paper does not address identity claims as meant in RFC 4949 [31], which are similar to knowledge claims (assertions that an entity has a certain identity).

Second, I use the notion of access. In a digital context, the notion of access combines the idea of being able to get to digital assets ("the means or opportunity to approach or enter a place"), and the idea of being able to use them ("the right or opportunity to use or benefit from something"). So, access to data involves both being able to get to the data and being able to use them. In addition, there is the process of getting access to the data ("The process of obtaining or retrieving information stored in a computer's memory").[3] The use of access in this paper is similar to the definition in RFC 4949: "The ability and means to communicate with or otherwise interact with a system to use system resources either to handle information or to gain knowledge of the information the system contains." [31].

For both claims and access, a distinction can be made between the content and the process or activity. Content points to what is claimed or what is being accessed (similar to entries in an access control matrix); process points to what is being done in relation to the access claim. When abstracting from the means of access to the underlying claim, the latter is also referred to as claims-making [23].

In addition to being made, access claims can be redeemed. That is, in addition to stating the requested access, the actual achievement of such access constitutes the redeeming of the claim. This can happen through exploitation of vulnerabilities or social engineering, but also through successfully selling IoT devices or through data extracted via dark patterns in a service offered. Governments and government agencies, in addition, can claim access through regulation. Thus, whereas the content of the claim can be independent from the means of access, the notion of redeeming points to *how* the claim is realised in terms of getting access.

The key idea is that these concepts (access, claims, and claims-making) can provide a common vocabulary for analysing different discourses that are currently visible in relation to cybersecurity. Having set the stage with these concepts, we will first shift our attention to claims-making as a political activity. Second, we will address the content of the claim, i.e. the resources to which access is claimed. In this context, we will primarily look at the literature on natural resources and associated claims. Then, I will use and translate the associated insights around (a) claims-making as a political activity and (b) natural resources as a potential content of claims to make sense of claims to digital and social resources in cyber settings.

[2]Definitions from https://en.oxforddictionaries.com/definition/claims.
[3]Definitions from https://en.oxforddictionaries.com/definition/access.

4 CLAIMS AND POLITICS

Lindekilde [23] defines claims-making as "the process of performing or articulating claims that bear on someone else's interests". Lindekilde focuses mostly on the political arena as the environment for claims-making. According to Lindekilde, "political claims-making entails both the formulation of a political demand with a specific content (the claim), and the public staging of this demand (claims-making)".

Following Lindekilde, there are two actors involved in claims-making: the claimant and the addressee. Assuming the addressee is meant to be human (or at least institutional), Lindekilde seems to see claims-making primarily as an activity aimed at *someone*. Indeed, he speaks of an "audience" of claims. This is also suggested by the example activities given (demanding, protesting, criticising, blaming). In addition, Lindekilde focuses on claims in the public sphere, and bypasses hidden political claims as in voting and lobbying. Also, although the idea of claims originates from the legal domain (enforcing a right), Lindekilde acknowledges that only a small part of political claims are brought to court.

In the present work, I do not specifically consider the legality of claims. That is, for analysing claims-making processes, whether the claim is legal or not is less relevant than whether the claim is successful in the sense of enabling access. In fact, whether claims are or become legal is itself a result of (political) claims-making processes. Successful access claims and associated technological infrastructures may influence the outcome of such processes. Similarly, the addressee acknowledging the claim or consenting to it may be part of the claims-making process, but is not a fundamental requirement for success. Nevertheless, lack of consent may be a reason for challenging the claim at some point.

The question is to what extent Lindekilde's political notion of claims-making is adequate for claims-making in relation to access in cyberspace. What is valuable in the approach is the highlighting of the political nature of the claim. As pointed out above, how threats, security and access are articulated forms an important aspect of access claims in cyberspace. Indeed, for Lindekilde claims seem to be mostly verbal performances, and he signals a link with concepts such as framing. However, from the point of view of philosophy of technology and material culture, claims may be articulated in many different ways than in language, and they may be much more hidden than public speech acts. That is, claims may be made via (obscure) technological rather than verbal means, which is what hackers often do (but also service providers and opinion manipulators). In addition, even when the (public) articulation of claims is similar, *what* is being claimed can be very different, such as access to data, attention, etc. What is being claimed may also affect actors other than the addressee, leading to third-party involvement, e.g. when access to personal data is claimed from a service provider. The focus of Lindekilde on the public sphere, the articulation of the claim and the addressee or audience de-emphasises the *content* of the claim.

Figure 1: Grounded claims on the island of Inisheer, Ireland (picture by the author).

5 CLAIMS AND RESOURCES

Claims always point to some kind of content that is addressed by the claim. Whereas Lindekilde focuses on a human or institutional *addressee or audience*, the *content* of what is claimed may have a more material or technical character. In the realm of cybersecurity, this is typically digital content such as data, software, bandwidth, or control over some device. The digital assets to which access is claimed can be seen as *resources*.

Claims to resources have been analysed in other domains [13, 20], and this can serve as inspiration for treating access claims in cybersecurity. Analogous to the discussion for cyberspace and data access, scholars have pointed out the need for a focus on transparency of claims and associated processes in for example land ownership and water resource management. In particular, it is acknowledged that resources often face *competing* claims by different stakeholders. This is obviously the case in what we normally see as cyber breaches or incidents (system owners vs. hackers), but also in privacy (citizens vs. "surveillance capitalists") and fake news (traditional media vs. manipulators).

In the context of natural resources, Kronenburg García & van Dijk [20] distinguish between factual access to land and legitimised access to land in the form of property. That is, claiming access follows a process in which somewhat stable access situations are created, which can however change over time, not only because of for example selling the property, but also because of changing historical / political circumstances. "Thus, 'having property', like 'having access', should be seen as social positions that temporarily crystallise at particular historical conjunctures" [20]. Acts of appropriation, through the process of claims-making, can serve as a basis for ensuring access for shorter or longer periods, by legitimising the access.

Kronenburg García & van Dijk distinguish between three types of claims-making practices in relation to land: "'grounding claims' is the practice of inscribing or altering the landscape with visible markers connoting ownership [Figure 1]; 'talking claims' is when speech is used strategically to make, justify and contest claims; and 'representing claims' is when claims are represented on material objects (maps, title deeds) that are detached from the resource." They also discuss how claims can be contested, for example through destroying landmarks (grounded claims), counterarguments (talking claims), or alternative maps (representing claims). In the competition with other claims, claims may be stronger or weaker. Stronger claims typically require more work, such as for example land planted with crops, stronger framing of talking claims, or multiple contracts for representing claims.

The different types of practices may form the basis for legitimisation of access. In this context, property signals legitimised access claims [19, 29, 38]. Whereas (private) property entails exclusivity in physical resources, this does not necessarily need to be the case for digital ones (cf. intellectual property). That is, although the resources are excludable (one can deny access), they are not necessarily rivalrous (access by someone does not decrease the value of the resource for others). Contrary to resources in other domains, digital resources are not necessarily "scarce", in the sense that there is limited supply, and use by one stakeholder precludes use by another. Data can be used many times without affecting the use by others, and this is reflected in open data initiatives. However, the *exclusivity* of access can be scarce, and this is partly what access claims compete about. Indeed, control may be the more important concept here. In addition, data can be leveraged to claim access to other scarce resources, such as the attention of people

[21, 32], or their opinions. In the words of Simon [32]: "What information consumes is rather obvious: it consumes the attention of its recipients."

According to Kronenburg García & van Dijk, "[b]oth appropriation and accessing are about excluding others from use and benefit, the former in a legitimate way". Assuming the resources are known, the others will realise that they are being excluded from access. This is not necessarily the case with digital resources. Because in the digital world scarcity of information is not the main issue, one does not need to have exclusivity to benefit, and claims need not be made visible as with land ownership. For attention, which is scarce, explicitly claiming (exclusive) access does not seem to be a feasible strategy. Indeed, rather than having people sign up for using a service for a minimum number of hours per week, they are persuaded into using it for longer periods. Thus, whereas it is quite hard to use someone else's land without this being visible, claims to digital resources can be kept completely secret (such as in Advanced Persistent Threats, for example (alleged) espionage through telephone network equipment). Even when users' attention is the main resource to be claimed (social resources), this can be kept subconscious.

So, in addition to the three types of claims discussed, we have a fourth type, constituting hidden or secret claims, in which there is no explicit representation of the claim. This includes claims for which the claimant actively suppresses such representations to prevent discovery of the claim (and possible contestation). In the following, we will speak of *covert claims*, as opposed to overt (or public) ones. Property only makes sense for claims that are public, and therefore require legitimisation. If data is accessed (only) through covert claims and means, there is no property relation involved, because the claims have not been (and most likely cannot be) legitimised. In fact, simply taking things, and associated allegations of theft, can be forms of covert claims regarding ownership [6]. Because covert claims are never explicitly made, they may be "harder to identify and resist" [39].

In addition to claims remaining hidden, resources may not necessarily be easily identifiable either. It is not always obvious that something is a resource that can be claimed. First, it needs to be understood as such; the phenomenon needs to be revealed as a resource [24]. If certain stakeholders recognise the "resource-ness" of a phenomenon first, without this being recognised by others, this clearly gives them a headstart in the claims-making process. As often said about new technological developments, government, regulation and ethics may lag behind what is going on in technological practice. (Covert) claims on yet unrecognised resources can be very strong, and may be embedded in infrastructures and practices before they even become contested.

In conclusion, access claims on resources involve a stakeholder, a resource, and a claim to that resource by the stakeholder. Different stakeholders may issue competing claims. Such claims may have different reasons, and support for the claim may be organised via speech, physical markings, representation, or (hidden) technological features. Finally, some kind of means gives actual access to the resource, backed up by the support. Compared to the earlier discussion of political claims-making, the focus is more on the *content* of the claims here rather than the process. Where political (public) claims-making emphasises addressees and legitimisation, the resources perspective emphasises which access is being claimed and how. Politics is just one of the possible means. Legitimisation is only possible if the claims are visible in the first place. For claims-making in cyberspace, both dimensions are important, because cybersecurity is politicised in its open manifestation, but many claims stay below the surface too. In fact, the quite different manifestations of claims could be one of the reasons for the disconnection of the several discourses.

6 THE LIFECYCLE OF ACCESS CLAIMS

As has been highlighted often for hacks, access claims go through different stages before being successful. In hacking, the Lockheed Martin kill chain model [18] distinguishes between reconnaissance, weaponisation, delivery, exploitation, installation, command & control, and actions on objectives. For claims, Kronenburg García & van Dijk mention appropriation, accessing and contestation as key phases. Most of the kill chain stages can be translated to claims-making as well, albeit in a slightly less technical interpretation. Kronenburg García & van Dijk look beyond the success of the claim, and this invites us to consider what may happen to access claims when they are challenged.

Combining the two views, I provide an initial sketch of stages that seem relevant when analysing different types of access claims.

Initiation and support. The "kill chain" of access claims starts out with someone preparing a claim and doing reconnaissance of the possibilities. This involves identifying something as a resource worth accessing, and figuring out how this could be done. A plan is made (involving grounding, talking, representing, or hiding), and actions are initiated. Technologies and people are mobilised to support the claim. This may include opportunities for "chained claims", i.e. someone may claim access to a resource from someone who has already successfully claimed access. Whereas some form of legitimation is necessary for overt claims, covert claims may receive support without legitimation, for example through technical means (e.g. selling IoT devices).

Note that claims may start from an existing relation between the claimant and the addressee, or building a relation may be part of the initiation and support stage. When a relation already exists, existing agreements or habits may support the new claim, such as when a new feature with access to a new type of data is added to a service. When a new relation is built, an overt claim may be part of a larger agreement, in which both parties may get something and give something. In both existing and new relations, trying to get consent for the claim could be part of the claims-making strategy. The transparency of such a process may vary (informed consent vs. dark patterns).

Initial access. This support may finally lead to a successful claim, granting access to the resource (i.e. redeeming). Again, for covert claims this may happen without legitimation of the claim in the public sphere. This success then enables exploiting the resulting access in order to do something with the resource.

Crystallisation (in technology), normalisation (in society). When access claims are successful, they become embedded in technological infrastructures. Because the different supporting actors – both

human/organisational and technological – "merge" into a stable network, one could say that "black boxes" are constructed around access claims. The claims become normalised, both in the sense of representation and legitimation, but also grounded in technology. This may also make initially overt or verbal claims less visible. These blackboxed claims may hinder competing claims, as transparency and contestation require explicit claims rather than blackboxed ones. In addition, stakeholders may try to create a regime under which they have default access to some resources, forcing other stakeholders to explicitly impose constraints if they find this undesirable. For example, with centralised solutions or platforms, providers have access to all information by default.

Operation. During their operative phase, access claims provide their associated benefits to the originating stakeholders. In this phase, access claims also act as constraints: they restrain what is possible in the future. When access is realised, temporarily or permanently, the associated resources can be utilised by the stakeholder that obtains access. Depending on the type of access, this possibility of use often limits other stakeholders in their action possibilities. With merely read access, others can still make use of the resource, but with full control this may not be the case. Realisation of access may also create path dependencies that make it harder to change the course of developments. For example, once the "standard" for IoT devices has been set in terms of continuous communication with the service provider, without significant protest, changing IoT into a more privacy-friendly direction will be difficult. In case of data, future read access to the resource can be secured by making copies, even if the access claim is only temporarily successful. In this way, access shapes future possibilities via constraints. Or, following the work of Grunwald [15], access implies a transformation of possibility spaces.

Contestation and rejection. When challenged / contested, possibly after first having been made visible, access claims may finally be rejected or otherwise stop existing. Claims can be challenged at any point in their lifecycle. For example, the mobilisation of support for a claim may be disrupted, the initial access may be blocked, and claims may be challenged before they become crystallised in technology. Even when in full operation claims may become contested, for example through investigative journalism sparking opposition.

Contestation and rejection also covers the issue of dispute resolution. While exclusivity of resources is not necessarily an issue, conflicts may still arise, leading to contestation of access claims. In particular, claims that are said to infringe on someone's rights (such as privacy) could be brought to court. Existing technological infrastructures and social norms may influence the outcome of such processes, begging the question to what extent technology itself regulates access claims. Emotions will also play a role in disputes on access claims, and may either be seen as irrational responses or as signals of the issues at stake [28].

In order to challenge a hidden claim, it first needs to be made visible/explicit. When a claim is challenged successfully, it may at some point be rejected. However, depending on its embedding in infrastructures and dependencies, revoking the established access may take a (very) long time. Some claims become contested heavily and early (smart meters and provider access to electricity usage data), whereas others hardly seem to be contested at all (digital TV and associated provider access to channel/program selection).

The later the stage in the lifecycle, the more difficult it becomes to change the access situation (reject the claim), because the support, crystallisation in technology, and normalisation in society have become more rigid. In addition, while the claim by a certain stakeholder to a resource may be challenged, other stakeholders may also have obtained access via claims addressed to this stakeholder, making it more difficult to revert the access. This is related to the Collingridge dilemma: the more we get to know about how a technology (access claim) operates, the more difficult it becomes to steer the development through interventions (contest/reject the claim) [7, 22]. This also implies that prescriptive use of the analytic framework outlined here may be challenging: it is difficult to do a sufficiently in-depth analysis of the actual claims-making processes compared to what is found desirable at a time when interventions are also still feasible.

Note that the outline above assumes that the access achieved is intentional. In fact, access may occur as a side-effect of other activities. Think of finding a dongle on a train. It is then up to the stakeholder involved whether this access is actually claimed, or whether the claim is rejected and the associated possibility of access given up. At a larger scale, there may be cases in which tech companies had not realised the value of some of the data they collected until they actually had it.

We have now defined the key concepts, identified how the notion of claims-making provides an analytical framework for natural resources, identified what needs to be added to make this framework suitable in the digital sphere, and described different stages in the claims-making process. Next, we'll summarise the analytical benefits and research possibilities, and then turn to some application scenarios.

7 ANALYTICAL CONTRIBUTIONS

The approach to analysis of cybersecurity issues in terms of claims-making provides several analytical benefits.

- It connects various discourses in the digital domain under the common denominator of access claims. Providing a social media platform, hacking it, and using it to distribute fake news all constitute access claims;
- It distinguishes between different means (grounding, talking, representing, hiding) to achieve the same goal (access), and explicitly adds covert claims as an endemic type of claim for digital resources;
- It emphasises the lifecycle for all types of access claims around digital resources, generalising stages in obtaining access (killchain-like approaches) beyond cyberattacks;
- Analysing claims-making processes postpones the question whether a specific type of access is legitimate / ethical / necessary / etc. First it identifies all the access claims. Then it investigates the implications of those access claims for future possibilities.

A remaining question is what kind of research can be done based on this framework. Giller et al. [13] provide some directions. In order to address competing resource claims in science, Giller et al. focus

on the following: "(i) the understanding of competing claims and stakeholder objectives; (ii) the identification of alternative resource use options, and (iii) the scientific support to negotiation processes between stakeholders". In this context, and following paradigms from science and technology studies, they see science itself as an arena of negotiation, and they see scientists as contributors to negotiation processes both within science (facts) and in the world (resources).

Giller et al. outline four main scientific activity areas around competing resource claims: describe, explain, explore, and design. Each of these areas comes with a more detailed set of possible scientific questions and associated activities. For descriptive research, the focus is on the current resources and claims in a domain, the drivers for these claims, existing institutional arrangements, and knowledge gaps. For explanatory research, the focus is on underlying processes and their role in changing resource dynamics. For explorative research, the focus is on extrapolating towards future scenarios. For interdisciplinary design research, the focus is on possible fixes for problems.

Thus, the analytical lens of claims-making and its benefits can be applied in different types of research, aimed at understanding and improving the *status quo* of access claims and claims-making activities. This lens needs to be applied to a reasonable scope in order to keep the analysis manageable. Especially in situations where claims are chained (a company claims data from a platform that has claimed it from users), or similarly where the addressee of the claim is not the owner of the resource, following all claims and all stakeholders involved may quickly yield a very complex picture. Setting a scope may limit the analysis based on the resources to be covered, the stakeholders to be included, the types of claims, etc., depending on the purpose of the analysis.

For claims-making analysis in cybersecurity, the following topics seem to be key in relation to the activity areas:

Describe What is the scope of the analysis? In this scope, what access is currently realised by which stakeholders? What are the underlying claims and their characteristics? How have the claims-making processes operated? Historical analysis and associated methods play a key role in answering these questions, most likely targeting stakeholders and their views, documents, as well as technological properties of the infrastructure.

Explain How are the current claims supported? Which structural characteristics (culture, law, institutions, technological platforms, ...) can explain the existing situation of access claims? Sociological and ethnographic methods may help with these questions. The concept of power may play a role here.

Explore How could the situation develop? What is the impact on ethical values? What are the normative issues involved? Futurists and ethicists can contribute to this type of research by investigating possible scenarios and their relation to values.

Design What structural properties could be changed to improve the impact of the access claims in the domain studied? These questions require an interdisciplinary design approach for socio-technical systems.

8 CASES

Below, the approach is illustrated for the cases of IoT and fake news. These cases were selected as illustrative examples for claims on digital and social resources, respectively, without asserting that they are representative of a larger class of phenomena. I do not claim to cover the full analysis possibilities as described above, which also means that the examples are at a fairly high level of abstraction. The focus is on what can be highlighted with the conceptual framework; some pointers for future-oriented research possibilities are also provided.

8.1 IoT

In the research presented in this paper, I originally started out by observing that in the Internet-of-Things, not all access claims are treated equally. Although security of IoT devices against access claims by hackers is no doubt important, many access claims in the Internet-of-Things are due to a transition from products to services. Whereas producers used to have no business in how we used our devices, this is changing with the current generation of devices that "phones home", informs the provider about our behaviour, and enables the provider to change functionality. This access claim is fundamentally not very different from a hacker claiming access to a system, although the strategy to enforce the claim is different.

In IoT, the key stakeholders issuing access claims (initiation and support stage) appear to be the users, the technology providers, and potential hackers/crackers. Key resources involved are user data and control of the devices. All claims except the user's are hidden in this case; whereas the user openly purchases devices, both providers and hackers do not have incentives to "talk" their access claims in public. Nonetheless, one could say that the claims are "grounded" in the software of the devices and the servers they talk to. In some sense, claims are also "represented" in terms and conditions for use, but these representations may not be effective in making the claims public. Support for access claims is mobilised by having the device "phone home" via its connectivity (providers), or via investigation of technical or social vulnerabilities (hacker). This support then enables redeeming of the claims and actually realising access (initial access stage).

In order to list the different claims involved, we focus on the following key characteristics, as discussed in the conclusion of Section 5: stakeholder, resource, reason, claim, support, and means. Table 1 provides an overview of stakeholders and claims. Note that in the table the claims are stated in terms of "need". While from the perspective of the issuing stakeholder it may actually be a desire ("want"), the claim may rather be talked in terms of "need" to provide sufficiently convincing argumentation.

For IoT, access claims by providers seem to have become normalised (crystallisation/normalisation stage), in the sense that it is accepted that providers of IoT devices get access to usage data. This access is also embedded in the technology (crystallisation). These normalised claims act as constraints on future developments, in the sense that while these claims are invisible, there is little incentive for new players on the market to start selling devices that don't carry similar claims. A key question around the future of IoT access claims is whether this centralised model, involving access claims of providers to usage data, is still amenable to contestation and

Table 1: Characteristics of access claims for IoT

Stakeholder	Resource	Reason	Claim	Support	Means
User	Smart control of device	Convenience	Need smart access to device	Purchase IoT device	App or other form of control
Provider	User / usage data	Mining, personalisation, profiling, sale	Need access to user/usage data	Sell IoT devices; get user consent	Device "phones home"
Hacker/cracker	Bandwith (DDoS), user data	Disruption, financial gain	Need access to devices / data	Find vulnerabilities / design persuasive communication	Exploit vulnerabilities / social engineer
Provider	Device software / firmware	Push updates/patches	Need to be able to change firmware	Frame as required for security reasons	Automatic update feature

change (contestation and rejection stage). That is, if we believe the access granted to the providers is excessive, and we wish to contest it, what could be done? Explorative research, e.g. into more decentralised models, could play a role here. However, if there are no incentives to actually adopt such an approach, technology itself will not solve the problem. At the very least, the current situation around access claims needs to be made more explicit in order for incentives to be created and for policy interventions to get support.

8.2 Online manipulation / fake news

Whereas in the IoT case, the *content* of the access claim is digital, there are several examples in which access to something non-digital can be claimed through digital *processes*. This is what happens in social manipulation through technology, this year's NSPW theme. Here, the key stakeholders are the user, the service provider seeking access to social resources (attention) to sell ads, and political actors seeking access to social resources to change opinions. In Table 2, an overview is provided of stakeholders and claims in the fake news "hack".

The social manipulation issue seems to have been created by some stakeholders identifying social resources before others, thereby enabling them to claim access first (initiation and support stage). By recognising the possibility of exploiting the resource via digital means, support could be organised via the different enabling platforms before the need for intervention became apparent. This then enabled redeeming the claim through the first instances of actual manipulation (initial access stage). Although the claims are clearly being challenged, the technological features that enable these claims have crystallised much more (normalisation/crystallisation stage). In fact, the possibility of manipulation seems to be strongly embedded ("grounded") in the service providers' own claim to user attention. While (self)-regulation is lagging behind, policy makers and platform providers struggle to find ways to make the adversarial access claims to social resources (manipulation) less effective and subject to contestation (contestation and rejection stage).

In the fake news discussion, we now see that some stakeholders are blamed for facilitating access claims by others: social media platforms are blamed for facilitating access to the social resources represented by their user base, thereby enabling chained claims that are not directly addressed to the owner of the resource. We see the same structure in quite some other phenomena, from early discussions on copyright infringement through file sharing to current discussions on hosting violent or otherwise problematic material. This is in itself a claims-making activity, namely in terms of government claiming access to platforms in order to control certain phenomena, in this case via overt ("talking") claims.

A particular issue here is whether technologies create new inequalities in access, facilitating access claims by some but not others. The concept of "bias" is relevant here: if technologies or platforms are biased towards access claims by certain stakeholders, their political role becomes profound. This in turn invites the disadvantaged to challenge these access claims and the underlying biases. We see increasing developments around challenging technological bias, but whether "unbiased" technology can be built or is even conceptually feasible is unclear. If technology cannot be neutral, equal access is infeasible *a priori*.

Also, the notion of distraction plays a role in this case, because what services seem to be about (sharing information and experiences) may be different from the resources that are actually of interest (profiles and attention). This may contribute to claims remaining obscure in the initial stages, enabling crystallisation before the claims become contested. Like in the IoT case, explication of the claims and associated issues may help to some extent in paving the way for (decentralised) alternatives. Interventions in the existing platforms could be possible, but run the risk of being seen as biased themselves.

9 CONCLUSIONS AND DISCUSSION

As outlined in the introduction, the idea to focus on access as a key analytical concept started from the situation in IoT, where threat models focused on hackers and threat models focused on providers didn't seem to "talk". In fact, the plan to write something about the philosophy of cybersecurity in relation to access was even older, inspired by the work of Floridi [9].

When finally committing to the topic for NSPW2019, it became clear that there is quite a range of literature on access claims in other domains, involving other types of resources, primarily natural ones. It seemed to make sense to connect this literature to what is happening in the digital security (and privacy) space. Especially in relation to the NSPW theme of this year, it appeared

Table 2: Characteristics of access claims for fake news

Stakeholder	Resource	Reason	Claim	Support	Means
User	News	Entertainment, opinion formation	Need access to news	Sign up for social media	App / website
Social media service	User attention and engagement	Selling advertisements	Need user attention	Provide sensational and personalised content	Get many users and keep them watching
Political actor	Citizen opinions	Political support	Need to change opinions / recruit support	Design attractive and fake content	Distribute content

that the notion of access claims and the analysis of claims-making processes provides a common denominator for the different (and rather disconnected) discussions. In addition, the notion of social manipulation through technology extends the claims concept from digital resources to social resources. In fact, critics of surveillance capitalism refer to the use of people as resources as a key characteristic of the developments, e.g. by framing the data collection activities as "people farming".[4]

In this context, the central hypothesis of this paper was that the notion of access claims provides a more general lens to study such phenomena than focusing on specific threats and specific means of access. I have tried to show through concept development and examples how this could work when analysing phenomena of access in cyberspace. In particular, I have linked the associated access claims to and contrasted them with claims-making activities in the political sphere, as well as claims to access to land as a natural resource. The examples of IoT and fake news illustrated the application of the analysis to digital resources and social resources, respectively. They also highlighted specific topics that may appear in a claims-making analysis, such as incentives, bias, and distraction.

Access claims in cyberspace have a political dimension, but they may also operate outside the public sphere in the form of covert claims and associated mechanisms, as in traditional hacks or access acquired through service provisioning. These claims do not only provide access to data, but also to behaviour of people and thereby some form of social control. Thus, social manipulation through technology can be analysed in terms of (often hidden, non-legitimised) access claims to social resources, and the associated redeeming mechanisms.

Despite the title, this paper is not about trying to use the technical hacking metaphor for manipulation of people (cf. [16]). Hacking is only used here to signal creative ways of claiming and gaining access, which can be done for any type of resource, not just digital ones. "Everything-as-a-Hack", then, is a paradigm in which gaining access via claims-making and redeeming is foregrounded as an analytical lens for various types of phenomena, including access to digital, physical and social resources, and the associated discussions. It does not imply ontological claims about the characteristics of such resources.

In addition to bringing separate discourses together, the focus on access claims foregrounds the political nature of security [8, 12] and its role in access to resources. Security is always security-for-someone and security-against-someone. Security politics decides who is a threat and who isn't, and which access claims are acceptable. Access claims can be problematised (such as those of hackers), normalised (such as those of intelligence agencies), or hidden (such as those of service providers). In such a context, "security-by-design" becomes a problematic concept, because it does not necessarily take into account the normalisation processes that have informed a specific definition of security. This also means that we get stuck in specific solution frames. The individualistic framing of privacy solutions in terms of user consent is an example of such a problematic frame. It doesn't fundamentally contest the access claims by the providers.

There is also a connection here with the application of actor-network theory to cybersecurity [37]. In actor-network theory, it is always a composition of different types of "actants" that acts. Similarly, it is not only a human actor that issues a claim, but a conglomerate of humans, technologies, and documents. Threat models and claims become embedded in infrastructures, leading to grounded claims that become increasingly strong. Technology helps to fix or crystallise the normalised access claims. Claims, social structures and technological structures form a complex socio-technical system that is difficult to disentangle. One could say that "cyborgs" or "black boxes" are created around such claims, hiding their presence and/or making it more difficult to challenge them. The question then becomes who is actually the originator of the claim. Seeing access claims as something issued by a conglomerate of different types of entities may provide conceptual benefits over conceiving claims as human (and organisational) business alone.

One could consider generalising claims beyond requests for access by the stakeholder concerned. While this is in a way the standard format, at least for natural resources, stakeholders may also explicitly ask to limit access by others. That is, (a) claims could be made by one stakeholder on behalf of another, and (b) claims could involve denying access in addition to granting access. So, one stakeholder could issue a claim requesting to grant or deny access to another stakeholder. For example, a privacy NGO could make a claim to deny an intelligence agency access to Internet usage data. The general format of claims would then look like "Stakeholder X should be granted/denied access to resource Y". Claims might also be bound to time (access for how long) and might include possibilities for delegation of access. Delegation introduces the concept of indirect access: someone claims access to data, and then gives the

[4] https://2018.ar.al/notes/we-didnt-lose-control-it-was-stolen/, consulted April 12, 2019.

data to someone else. This may not necessarily be a claim by the third party; instead, access is being claimed on behalf of someone else. Claims could be issued (or made explicit) after-the-fact, such as in coverage of incidents (who had access and why) or in break-the-glass scenarios (who broke the glass and why). Literature on argumentation may provide useful inputs for studying the structure of claims, including such generalisations [26, 35]. How this plays out in specific discourses / themes could be investigated further.

It seems that the idea of claiming access also suggests the idea of counter-claims, especially when considering the generalisation including denial of access as mentioned above. That is, security controls could represent counter-claims against access claims by others. Another example of a counter-claim would be the revocation of (claimed) access. Control is important here: a counter-claim can only be effective if the access situation can actually be influenced. If data has spread all over the Internet, revoking access in a particular platform may not be effective. Again, there is a link with the argumentation literature here, to the extent that counter-claims are similar to counterarguments.

On the content side of claims, the notion of "capital" could also play a role in describing the resources that are being accessed. In fact, there is recent work on introducing the notion of "semantic capital" in addition to economic, social, and other forms of capital [10]. In this line of reasoning, the issues with threat models and access claims have a lot to do with (threats to) the distribution of different types of capital in society. Digital technologies enable new types of access claims to all types of capital, including economic (platforms), social (manipulation) and semantic (data).

Interestingly, as pointed out by one of the reviewers, suggesting to reveal access claims is itself an access claim as well, and constitutes a political activity. That is, the framework outlined in this paper is not necessarily a neutral scientific tool, but fits better within critical theory, in the sense that it reflects on and criticises the current state of affairs in society. In particular, the framework is critical of the present situation in which access claims by powerful actors remain obscure. Indeed, this implies that it should also reflect on its own claims, and make those explicit. The claim of access articulated in the present paper, then, can be said to be aimed at access to access claims, and put forward by a single author, to be evaluated by the scientific community. The amount of support and associated means of redeeming the claim are still uncertain.

In the present paper, I have outlined the analytical focus on access claims and claims-making processes, both in claims on digital resources and in claims on social resources via digital means. I have illustrated the approach by cases on IoT and fake news, highlighting some of the specificities of access claims in these phenomena. As a general conclusion, I believe that access claims and claims-making processes are useful analytical tools to compare different discussions that are somehow related to cybersecurity, but currently not fully connected. I'm happy to have claimed access to NSPW2019 to develop these ideas further.

Acknowledgments

Thanks to Jonathan Spring, Tom Walcott, Mary-Ellen Zurko, and NSPW reviewers and participants for valuable comments.

REFERENCES

[1] Richard Barber. Hackers profiled – who are they and what are their motivations? *Computer Fraud & Security*, 2001(2):14–17, 2001.
[2] Peter L. Berger and Thomas Luckmann. *The social construction of reality: A treatise in the sociology of knowledge*. Penguin UK, 1991.
[3] Hal Berghel. Software sophistry and political sleight of hand. *Computer*, 50(1):82–87, Jan 2017.
[4] Matt Bishop. The insider problem revisited. In *Proceedings of the 2005 New Security Paradigms Workshop*, NSPW '05, pages 75–76, New York, NY, USA, 2005. ACM.
[5] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, 2016(4):237–254, 2016.
[6] James Carrier. Property and social relations in Melanesian anthropology. In C. Hann, editor, *Property relations: Renewing the anthropological tradition*, pages 85–103. Cambridge University Press Cambridge, UK, 1998.
[7] David Collingridge. *The social control of technology*. St Martin, New York, 1980.
[8] Laura Fichtner, Wolter Pieters, and André Teixeira. Cybersecurity as a politikum: Implications of security discourses for infrastructures. In *Proceedings of the 2016 New Security Paradigms Workshop*, NSPW '16, pages 36–48, New York, NY, USA, 2016. ACM.
[9] Luciano Floridi. The ontological interpretation of informational privacy. *Ethics and Information Technology*, 7:185–200, 2005.
[10] Luciano Floridi. Semantic capital: Its nature, value, and curation. *Philosophy & Technology*, 31(4):481–497, 2018.
[11] Virginia N. L. Franqueira, André van Cleeff, Pascal van Eck, and Roel Wieringa. External insider threat: A real security challenge in enterprise value webs. In *2010 International Conference on Availability, Reliability and Security*, pages 446–453, 2010.
[12] Dan Geer. Cybersecurity as realpolitik. Black Hat USA, http://geer.tinho.net/geer.blackhat.6viii14.txt, 2014.
[13] Ken E. Giller, Cees Leeuwis, Jens A. Andersson, Wim Andriesse, Arie Brouwer, P.G.H. Frost, P.G.M. Hebinck, I.M.A. Heitkönig, Martin K. Van Ittersum, N.B.J. Koning, et al. Competing claims on natural resources: what role for science? *Ecology and society*, 13(2), 2008.
[14] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. The dark (patterns) side of UX design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, page 534. ACM, 2018.
[15] Armin Grunwald. Technik als Transformation von Möglichkeitsräumen. Technikphilosophie anders gedacht. In *Möglichkeiten der Reflexion: Festschrift für Christoph Hubig*, page 203. Nomos Verlag, 2018.
[16] Yuval Noah Harari. *Homo Deus: A brief history of tomorrow*. Random House, 2016.
[17] Cormac Herley and Wolter Pieters. "If you were attacked, you'd be sorry": Counterfactuals as security arguments. In *Proceedings of the 2015 New Security Paradigms Workshop*, NSPW '15, pages 112–123, New York, NY, USA, 2015. ACM.
[18] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In *Proceedings 6th International Conference Information Warfare and Security (ICIW 11)*, pages 113–125, 2011.
[19] Nicola Jentzsch. Dateneigentum – Eine gute Idee für die Datenökonomie? Stiftung Neue Verantwortung, https://www.stiftung-nv.de/sites/default/files/nicola_jentzsch_dateneigentum.pdf, 2018.
[20] Angela Kronenburg García and Han van Dijk. Towards a theory of claim making: Bridging access and property theory. *Society & Natural Resources*, doi: 10.1080/08941920.2018.1559381, 2019.
[21] Richard A. Lanham. *The economics of attention: Style and substance in the age of information*. University of Chicago Press, 2006.
[22] Wolfgang Liebert and Jan C. Schmidt. Collingridge's dilemma and technoscience. *Poiesis & Praxis*, 7(1-2):55–71, 2010.
[23] Lasse Lindekilde. Claims-making. In *The Wiley-Blackwell Encyclopedia of Social and Political Movements*. 2013.
[24] Wolter Pieters. Reve{a,i}ling the risks: a phenomenology of information security. *Techné: Research in Philosophy and Technology*, 14(3):176–188, 2010.
[25] Wolter Pieters and Luca Consoli. Vulnerabilities and responsibilities: dealing with monsters in computer security. *Journal of Information, Communication and Ethics in Society*, 7(4):243–257, 2009.
[26] Henry Prakken, Dan Ionita, and Roel Wieringa. Risk assessment as an argumentation game. In J. Leite, T. Son, P. Torroni, L. van der Torre, and S. Woltran, editors, *Computational Logic in Multi-Agent Systems*, volume 8143 of *Lecture Notes in Computer Science*, pages 357–373. Springer Berlin Heidelberg, 2013.
[27] Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, and Matt Bishop. Aspects of insider threats. In Christian W. Probst, Jeffrey Hunker, Dieter Gollmann, and Matt Bishop, editors, *Insider Threats in Cyber Security*, pages 1–15. Springer US, Boston, MA, 2010.
[28] Sabine Roeser. The role of emotions in judging the moral acceptability of risks. *Safety Science*, 44(8):689–700, 2006.
[29] Paul M. Schwartz. Property, privacy, and personal data. *Harv. L. Rev.*, 117:2056, 2003.

[30] Eric D. Shaw, Keven G. Ruby, and Jerrold M. Post. The insider threat to information systems. *Security Awareness Bulletin*, 98(2):1–10, 1998.
[31] Robert W. Shirey. RFC 4949-Internet Security Glossary. Available online: https://tools.ietf.org/html/rfc4949, 2007.
[32] Herbert A. Simon. Designing organizations for an information-rich world. In M. Greenberger, editor, *Computers, Communication, and the Public Interest*. Johns Hopkins Press, Baltimore, MD, 1971.
[33] Johan Söderberg. Misuser inventions and the invention of the misuser: Hackers, crackers and filesharers. *Science as culture*, 19(2):151–179, 2010.
[34] Nick Srnicek. The challenges of platform capitalism: Understanding the logic of a new business model. *Juncture*, 23(4):254–257, 2017.
[35] Stephen E. Toulmin. *The Uses of Argument*. Cambridge University Press, Cambridge, UK, 1958.
[36] Orly Turgeman-Goldschmidt. Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology*, 2(2):382–396, 2008.
[37] Wytske van der Wagen and Wolter Pieters. From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. *British Journal of Criminology*, 55(3):578–595, 2015.
[38] Jeremy Waldron. Property and ownership. In Edward N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, winter 2016 edition, 2016.
[39] Michael Warren. Religious formation in the context of social formation. *Religious education*, 82(4):515–528, 1987.
[40] Shoshana Zuboff. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1):75–89, 2015.