Ethical considerations in sharing cyber threat intelligence

Siri Bromander
mnemonic as
University of Oslo (UiO), Norway
siri@mnemonic.no

Abstract

Sharing information with others is always a choice. In the world of cyber defense, sharing information with others can help others defend themselves, and with this increase the joint defense our society needs to have in order to stay safe. Several factors influences the choice of sharing valuable cyber threat intelligence, and the ethical considerations are argued to be a prominent part of this.

When encountering a situation where a choice of sharing information is emerging, the choice will be twofold: 1. what information should be shared?, and 2. with whom should the information be shared? The ethical challenges of the choices is primarily tied to who you have obligations to. The consequences of the choices will potentially affect the society in variable degrees, your employer, your colleagues, your friends and obviously yourself.

This article discusses the ethical considerations cyber security personnel is facing making these types of decisions.

The first part of the article explains details of cyber threat intelligence and its community architecture. Following this, the article describes what influences the choice personnel is facing when having the possibility to share valuable information with others, tying the considerations to known research within knowledge management and ethics of knowledge sharing. An example is given to discuss the possible choices and the ethical considerations within all possible choices. Towards the end a short note is done on sharing information in the aftermath of incidents instead of during an incident. The articles concludes that not sharing valuable information at all is immoral, but how much and with whom needs to be a consideration made special in each case, leaving a deontological approach unsuitable.

1 Cyber Threat Intelligence

Cyber infrastructure encompasses many aspects of our daily lives. Our homes are an increasing part of the 'Internet of Things', our society is increasingly digitalized and

This paper was presented at the NIK-2017 conference; see http://www.nik.no/.

our workplaces are all, to some degree, using available cloud services as convenient and efficient solutions for us to perform at our best. Everything connected to the internet is made available to the rest of the world. The rest of the world are not always having only good intentions. Everything available on the internet makes possible targets for cyber threats[1], and the consequences are possibly lethal; physical damage to for example a dam or a nuclear power plant could kill numerous people and provide environmental changes beyond repair within our lifetime. Defending ourselves has never been more important, and will be increasingly important in the years to come.

Cyber-attacks are becoming more common, sophisticated and damaging. The stories of Stuxnet, the 2016 US Election and the more recent ransomware WannaCry reveals the concerning fact that highly skilled threat agents are capable of sabotage, espionage and subversion to the degree of nation state concern. Some argue there is no such thing as cyber warfare[1], but in July 2016 NATO recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea[2]. The terminology used may not be as interesting as the discussion revealing capabilities and consequences of conflict in the field of cyber. Recent history shows us that critical infrastructure can be taken down, elections may be influenced and critical parts of society can be disrupted for days caused by attacks happening in cyber space alone.

The need for advanced and rapid response is increasing. Seeing the battlefield is far less visual than that of physical war, the need for sharing and communicating known intelligence between defending partners increase. Sharing information and knowledge is a field of its own. A field where technical and strategic obstacles are discussed and debated, but where I would argue that ethical considerations are just as important to address.

Cyber threat intelligence started out as something the larger and best computer incident response environments did to succeed in their day to day job. Good work made good results which could be useful to others trying to defend against the same adversary. To receive good information one needed to share good information, and so started the large communities of cyber threat intelligence. The commercial value of this type of work was quite fast seen by other environments, and the market for threat intelligence grew very fast[3]. Today we are facing a severe amount of businesses offering threat intelligence products.

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard[4]. In the world of cyber security, this means sharing everything from smaller network artifacts, indicators of compromise and samples of malware or infection vectors, to descriptions of how attackers are operating, their capabilities and intents. In some cases also the identity of attackers are shared. The format of sharing this type of information is going from emails, files and chat-channels, to automatic feeds. The timing of such sharing is often very important as much of the information shared is only valid for a limited amount of time and can be crucial to receive in order to be able to handle whatever threat is targeting you. More often than not is this type of sharing based on personal

[1] Oxford dictionary: 'Cyber threat: The possibility of a malicious attempt to damage or disrupt a computer network or system.'

relationships. The choice of what to share and who to share it with is often a decision made or at least initiated in the moment by the same personnel doing incident response and threat hunting activities.

The information we gain when investigating an incident in a thorough manner is knowledge, and knowledge management is a relatively young but evolved field of research. In relation to knowledge and business ethics it is seen that an unwillingness to share knowledge that may hurt an organization's survival is seen as being seriously unethical[5]. In general, we could argue that the knowledge you have about an adversary that may seriously injure another organization is something we are morally obliged to share, but in our circumstances the decision to share may also give the consequences of severely injuring your own ability to defend yourself against serious consequences. The debate is therefore somewhat more complex in our circumstances.

We need to look at the general facts and circumstances that will influence the choice of action when facing situations where sharing is an option.

The first aspects that will influence the decision you make is how knowledgeable the receiver of your information or knowledge is. If organizational members believe in other members' expertise and skills, the intention to share individual knowledge increases[6]. Often the use of shared threat intelligence can ruin the information itself, if the information you provide them is used in a manner the adversary is capable of detecting. 'Blowing' the intelligence received is seen as likely if the recipient has little knowledge or experience in both handling the technical details as well as the stress related to a serious incident. The intent is seldom to ruin the information when using it to defend yourself, but the possible consequences are nevertheless there.

Secondly, also related to knowledge, is the ability for managers to understand the consequences of sharing. Sharing is ultimately seen as a good deed, but sometimes information shared is carrying metadata which can reveal more than initially thought. This is something the technical personnel may try to explain to their managers, but not knowing the business sides missing to understand the consequences of and therefore not being able to explain in a sufficient way. The uncertainty of not knowing how much is actually revealed with sharing a given set of information, often influences the choice of sharing towards not sharing.

Thirdly, who can be affected by your decision is relevant, and how you are obliged to them. Working for a company most always encounter a contract of work, making you obliged to follow company policy and the instructions of your managers. Being a citizen of a given country you are obliged by law to follow the rules set in that country. As part of a volunteer community you are expected by your peers to contribute, and you may even owe someone in the community or elsewhere a favor after significant help in the past. In some cases you may be in a situation where certain others seems to deserve help as they are either a special type of organization or critical of nature, and the overall obligation to prevent bad behavior and criminal acts as part of the society is always present.

From knowledge management we know that knowledge alliances motivate managers to enter into strategic alliances with other firms in order to balance knowledge deficiencies, obtain necessary competencies and create new knowledge[7]. This is exemplified by cyber threat intelligence and the vast amounts of sharing and collaboration networks that exists. Some of these are based upon contracts and legal obligations, like reporting to governmental parties when handling critical

infrastructure, and some are just based on spoken agreements and the desire to share and collaborate like companies working in the same industry collaborating when it is found useful. Either way the collaboration agreements you are faced with will influence your choice of sharing information.

Fourthly, the culture of both the country, organization and community in which you reside affects the willingness to share knowledge. Ethical decision-making is affected by culture through an individual's deontological and teleological evaluations. Although individuals may regard a particular activity as ethical, they may follow a different course of action because of the desirable outcome. Because people make different assumptions about personal knowledge, it can therefore not be assumed that workers in all cultural value systems will view their own decision not to share their personal knowledge, or a decision to act out of self-interest in the face of internal competition, as unethical or immoral[6]. Within cyber threat intelligence, these challenges can be exemplified with the differences between corporate organizations and military organizations. Even though personnel from both have obligations to their residing country, military personnel would arguably act from a stronger obligation to national interests, simply because of their training, experience and choice of work place. Consequently, their evaluation of consequences on national security plays stronger than those of for example financial loss or personal gain.

Finally, timing is of importance. The nature of threat intelligence is that is most often is only valid for a limited amount of time, and that the receiver needs it as soon as possible to increase their ability to defend. An example is information on the infrastructure used for attacking a given organization. An advanced attacker would change the used infrastructure on a regular basis, leaving information on IP addresses and domains useless as soon as they swap. In many cases this is a matter of hours. Sometimes this means that there is not enough time to go all the rounds internally to get approval before you share, and also that the time spent on considering all consequences of the action could be a waste of time you do not have. Whether you share classified information when sharing, or whether the attacker is pushed to change its infrastructure sooner and leaves yourself unable to know where the attack is coming from next, are considerations that requires time consuming analysis. If conducting all analysis before sharing, the information may no longer be worth sharing. In these terms it could be argued that following rules, adhering to duties (deontological approach) is far better for the time sensitive matter of sharing threat intelligence than that of considering consequences.

2 An example: sharing while enforcing your own defense

A normal situation for a security analyst to be in is given as an example to illustrate the challenges related to deciding who to share with. The described situation illustrates the influencing factors relevant to the ethical consideration the analyst must make.

Imagine the scenario: you are a young security analyst, skilled and with experience from several organizations, both work related and as part of the volunteer security community. You are popular both because you are knowledgeable, but also because you on several occasions have helped others in succeeding with handling difficult incidents in the past. You are active within several cyber security communities on your spare time.

At work, you take place in the handling of a severe security incident. An adversary has successfully compromised your computer network, but you have detected the attacker and are monitoring their every move together with your team. You do not know for sure what the adversary is after, but based on the business of which your company is working, you have a fair idea. If your suspicion is right, the adversary in question would be able to do severe physical damage through your computer systems if not stopped. You have several friends in organizations likely to be targeted by the same adversary, both private and public sector, and the adversary is likely to be after valuables of national interests and capable of sabotaging critical infrastructure. You also know enough about the adversary to conclude it is an advanced attacker with the ability to change its behavior to the extent that you are no longer able to either detect or monitor them anymore. Hence you are depending on your knowledge not to be leaked to the adversary in any way to be sure you can defend against them yourself. You prepare information on how to detect and monitor the adversary for sharing with others and approach your manager. The discussion that follows is difficult: Should we share this information? And with whom? Who are we obliged to help and to what extent can we morally defend putting our own defense before others? Is personal obligations something you can set aside or is that relevant as well?

There are technical and practical aspects that we set aside for this discussion, like the ability to share the information in a relevant manner. For our purposed we are looking into the ethical aspects of the decision of sharing/not sharing with different parties.

To debate what is morally right and wrong in our example we need to examine the possible actions and related rules (deontological approach), and the consequences of our possible actions, both the direct consequences and the long term consequences (teleological approach, in this case consequentialism).

So the possible choices to make regarding our piece of information in this situation are the following:

- **Doing nothing.** A general, positive rule is that 'we share information that can help others'. In these terms the act of not sharing information is unethical. However, if sharing that information encounters possibly sharing metadata covered by laws and regulations in the county in question, you are breaking a more prominent rule of 'do not break national laws'. However, if skilled at incident response you know what information that is ok to share, and the deontological approach would tell you that the act of not sharing is unethical.

  The consequences of not sharing information is directly that you do not spend time on it, which may help you do better at actual defense. In addition, you are certain that you keep all company information safe. On the negative side you find several consequences, but the worst would be that several others are not able to defend themselves and that it could lead to severe physical damage. With this as considerations it is not ethically possible to defend not sharing information with anyone. I consider the action of 'waiting and sharing later' to give the same discussion as above.

- **Sharing information with national capabilities only.** In Norway (and most countries with defined national cyber capabilities) there are laws and regulations stating that incidents which can affect national security shall be

reported to the authorities. This means that handling an incident in your environment if your environment is part of for example critical infrastructure, is something that should be reported as soon as the incident has been detected. The decision of not helping anyone else does however mean you do break the rule of 'we share information that can help others' as stated above.

Company policies are usually having statements in lines of 'we shall always adhere to laws and regulations, but any circumstances where we suspect possible prosecution as a consequence shall be run by legal'. In the time sensitive circumstances of incident response, this often means you need to break either company or national laws when deciding. Most companies will officially state that national laws are first in line, but in real world scenarios we see that this is not always as straight forward. If considering our society it is hard to argue that not sharing with national capabilities is morally right.

If evaluating consequences the most prominent positive are that they can protect our national interest. They can decide on further sharing, which for many means you have done your duty. But knowing the authorities does not have the same network as yourself, you know that not everyone you could have helped is being helped. This is still breaking your obligations to the society and the security community and still many organizations being defenseless must be seen as a negative consequence still. Further, on negative side of actually sharing with the authorities, is the uncertainty of how well they will treat the information you provide them with. Their interests and their skill level is probably unknown to you, and you risk them ruining your own defense. The information you provide can put you in a position where they will investigate you further, and also, you risk that they will classify your information which makes it harder for you to use in the further.

Sharing with the authorities is seldom argued immoral due to the laws and their ability to help national interests, but not sharing with others may be defended as unethical.

- **Sharing information with those you know.** The situation where people that are close to you get hurt is harder to accept. The rule of helping others is strengthened, but will only survive as long as laws or regulations are not forbidding you to share information. Seeing you know those close to you, your evaluation of skill level is related to less uncertainty, which decreases the negative consequences of sharing with them. Breaking laws to share would encounter prosecution and would not be considered ethical if lives are not at stake. Following both deontological and teleological approaches will therefore likely give the same conclusion: you should share as long as the recipients are allowed to by law.

- **Sharing information with the relevant sectors.** Within the security industry several sharing collaborations has been created in order to share with relevant partners in different incidents. The groups are often created in different industry sectors and based on voluntary participation. It can be seen as closed sharing with participation restrictions, but without personal knowledge of the group of recipients, their skill level and where their loyalty lies.

In our example we have a situation where the analyst is not obliged by rule or formal contract to share. The rule of sharing information to help others is still present and I can find no other rule that is strong enough to contradict this. However, looking at the possible consequences of sharing you have larger degree of uncertainty related to how the information is being treated and therefore you have potential consequences ruining the information not only for you, but also for national capabilities and others you have shared with. Given this evaluation I find it to be defendable to limit the amount of sharing done to those you know can help the most and maybe can assume can handle the information best.

- **Sharing information with everyone.** The act of sharing information with everyone is good alone. It follows the rule of 'you are not keeping to yourself information that can be valuable to someone else'. Seeing it is impossible for you to know everyone who can gain value out of the information you share, broadcasting the information in ways that makes everyone interested capable of finding it is therefore the right way to go. Technically, this means creating a public report or similar and publishing it somewhere online. However, sharing with everyone also means sharing with your adversaries, and knowing this breaks the unwritten rule of 'not telling your enemies how you work or what you know'. Which rule is the most prominent of these? The uncertainty of the latter and the size of the benefit it serves other victims will judge this.

  Following the consequences of these actions, one can argue that the good of sharing with everyone is both that more people may be able to protect themselves, but also that by sharing intelligence more people can learn and the general skill level is increased. The flip side is as indicated earlier, the adversaries may change their patterns, improve and be even harder to protect against in the future[8].

  In these terms the 'doctrine of double effect' comes into relevance. If sharing the information with everybody, then it is likely that everyone will benefit in the short run, but the advanced communities will lose eyes on the adversary as soon at the adversary knows their details are known. This is known, but the good of more organizations being able to defend themselves in the short run, outweighs the fact that the adversary is able to escape detection by changing the details now known in the broader communities. This is seen as ethically defendable as long as the intention is that of helping more organization defending themselves, and not to help the adversaries in improving their methods.

3 Sharing information about past cyber incidents

Another relevant question concerns sharing information about a cyber-threat in the aftermath of an incident. This can still contain valuable information about an adversary, but often not technical information that can be of direct help to a certain incident. IP addresses are no longer in use by the adversary, but they still use the same procedures when attacking a new victim. Even though the technical details may be ruined and useless, information about cyber threat methodology stays robust over time and may be shared in the aftermaths of an incident to contribute to the base of experience the rest of the security communities can benefit from. The

information can therefore not be ruined by recipients that lacks sufficient knowledge. Also, to share information is often a decision made by others than the personnel themselves, for example marketing or legal, but is still an interesting and related debate to address. The consequences of such an action is less influenced by that of 'ruining information' and hence not as related to the knowledge of the recipients, but more so of the long term consequences of the community we live in. Sharing knowledge between defending parties makes our community better prepared and more likely able to protect its citizens. The conclusions made within knowledge management theory[5] is therefore more valid here, and it is possible to state that not sharing such knowledge is considered unethical.

4 Conclusions

The position you are in/the context will always influence the decision you make and also the difficulties of acting morally right. The most prominent aspects influencing the decision of sharing threat intelligence is who you are obliged to, who can be affected by your decision and how much damage the information can have among the wrong recipients. In our cyber security world we see that both employer and friends in the security community have high influence. Trust in and skillset of the recipients is of high importance when evaluating the possible consequences. When sharing sensitive information one needs to trust the recipient to protect it from the adversaries and not to ruin it. Sharing information itself is a good deed, but if the negative consequences are easily understood, then the decision not to share is the easiest. The ethical challenges of acting against laws and regulations seems to be the strongest positive influence on the choice of sharing information, which may come as a result of the little analysis needed to understand the consequence. The extent of both negative and positive consequences of sharing cyber threat intelligence is otherwise requiring more extensive analysis and may not be possible to even estimate due to time constraints and lack of available knowledge. Your assumed adversary may be able to severely damage your organization and your peers may be able to both use the received information and treat it with care. When uncertain people often has a tendency not to act.

Creating a given rule to follow in any such case is impossible due to the large degree of uncertainty in the above stated aspects influencing the choice of action. A solely deontological approach is therefore not a suitable ethical framework to deal with such cases.

As part of a society the long term consequences of not sharing information at all is making the act immoral. With the knowledge of severe negative consequences of sharing a piece of information, the sharing can defendable be done within closed communities where the recipients are known to treat the information right, like sector specific sharing groups or sharing with groups consisting of members based on 'invite only'. However, in the aftermath of an incident, when the incident has been handled, I can see no good argumentation to defend the act of not sharing valuable threat intelligence. The consequences of not sharing information or revealing real incidents will in the long run mean that less people understand the severity of the cyber-attacks in our region, and consequently do not spend resources protecting against them. For us as a society that is a major security issue.

References

[1] Thomas Rid. Cyber war will not take place. *Journal of strategic studies*, 35(1):5–32, 2012.

[2] NATO. Warsaw summit communiquÃ©. `https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf`, 2016.

[3] Brian Bartholomew and Juan Andres Guerrero-Saade. Wave your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks. In *Virus Bulletin Conference*, 2016.

[4] Gartner. Definition: Threat intelligence. `https://www.gartner.com/doc/2487216/definition-threat-intelligence`, 2013.

[5] Chieh-Peng Lin. To share or not to share: Modeling tacit knowledge sharing, its mediators and antecedents. *Journal of business ethics*, 70(4):411–428, 2007.

[6] Nina Evans and Mary McKinley. Ethical paradoxes in knowledge management. *Vie & sciences de l'entreprise*, (2):57–71, 2011.

[7] Richard Baskerville and Alina Dulipovici. The theoretical foundations of knowledge management. *Knowledge Management Research & Practice*, 4(2):83–105, 2006.

[8] Gadi Evron and Inbar Raz. Apt reports and opsec evolution, or: these are not the apt reports you are looking for. `https://www.virusbulletin.com/uploads/pdf/magazine/2017/VB2016-EvronRaz.pdf`, 2016.