WannaScry!
An Interview with Danja Vasiliev

Danja Vasiliev and Daniel Irrgang

Danja Vasiliev, co-author of "The Critical Engineering Manifesto," is an artist and activist working on the exposure of data exploitations in networked systems. The interview centres around his work "WannaScry!", an installation revealing privacy issues of video conference platforms and which was under development at the time this conversation took place (October 23, 2020).

Daniel Irrgang: I would like to start this conversation with a quote taken from a text you and Julian Oliver wrote for a book published by transmediale festival in 2016, which, in my view, frames the motivation behind your work: "Engineering is far too important to be left to the experts – to academic papers, patents, military and corporate research facilities … The cultural conversation we call art is challenging aesthetic, social, cultural, and political habits and regimes to better understand how we are their subjects. In today's world of integrated and automated systems, complex communication networks and their technologies, there is no less need for such subjective transformation. Only by doing so can new mobilities (and thus futures) be modelled. Without insulting from state intervention by art infrastructure, there would be no safe, public forum for techno-political expression, no context for understanding how our increasingly engineered environment engineers us. But a black box made of many" (Oliver and

Vasiliev 2018, 201). This quote contains references to privacy, digital literacy or digital sovereignty and the role that art and activism can play in exposing opaque power relations. Do you want to elaborate the premisses of both the quote and your work?

Danja Vasiliev: References are extensive, I guess. Probably the earliest one, historically speaking, is that we build machines by our own example. Such as the early fantasies we have of robots, of the expectations we have of machines in general, which I think are flawed, just as our expectations of other people are flawed. So, despite the fact that we create machines by our example, we create technology as a juxtaposition to the biological substrate. But to humanize machines is a big failure of our human-computer interaction model, I think. And it is something that new generations absorb as part of their upbringing. But people even today, in our age and in our circles, they have not been drawn to these machines like new generations have, and still, up to this day, we are wrapping our heads around this paradigm. We now have to trust and rely more and more on things that actually are artificial, things which make decisions based solely on algorithms.

I don't know if this relates much but going back to the quote, I think at the core of it all is the concern that, should we trust technology to be applied solely by governments and corporations, what we are going to get is a very police-like regulation, promoting types of technologies to keep society under a watchful eye.

At the same time, we are at a point where technology is so ubiquitous. There has to be a place for cultural experimentation to promote all these twists of our human minds, twists other than hurting or restricting our communities, such as curiosity-driven projects and different strands of research, they all have to have their place. Should we allow the technology to be policed and to be encapsulated in machines and products that dictate an already final, opaque and standardised design? This will end up destroying any opportunity for future culture to develop, because the assumption is more and more that culture will rely on underlying technology and thus, by extension, on the freedom that this technology affords or allows when it comes to altering, modifying and individually developing it.

And it has been an observation of multiple people in the field that the further technology develops towards complexity, the more opaque it gets – a factor that comes along with efficiency. So, the

more efficient technology is, the more black-boxed it will be, just by nature of having to integrate more and more circuits on a particular chip. A record player, with a spinning plate, a pickup and so on, is a good example of previous technology and a great analogy of a very extroverted device which tells you a lot about itself and how it works, compared to mobile phones or similar devices where it is often hard to tell what the designated functions of components are. It is more complicated, or even impossible, for new generations to decipher and understand all those elements. If you try to open such a black box you will probably break it, and no one will fix it for you.

Such considerations have a huge impact on how I do my work. It is very important to attempt to reclaim the ability to interact with technology, in a way that sometimes might even be illegal, to uncover the hidden principles of networked technologies. I hope this approach will be more and more discovered by different groups of people. Not to say that this is always discouraged, of course there are devices like Raspberry Pi and Arduino boards, but still it remains very difficult to approach an off-the-shelve consumer device, crack its cover open and attempt to mess with something that wasn't ever designed to be messed with. This is why the "Critical Engineering Manifesto" (Oliver, Savičić, and Vasiliev 2011–2019) was written all those years ago and why other people like you and around the world teach these ideas to their students.

DI: Historically it would be interesting to note that the claims you and others make, to open technological devices and to bend their circuits to our own will, cannot only be traced back to the hacking of ICT but has its roots far deeper. For example, the German Radio Workers Movement, which, especially in the 1930s, built their own radio transmitters to understand how this, back then new, media functioned, and to be able to distribute their own political messages, beyond the restricted and centralized political agenda of the government. Of course, these movements where quickly criminalized and suppressed as soon as the Nazi government came to power.

DV: Yes, some of them where even former military, that's why they had the skills and knowledge to carry some of that technology into the public sphere. They were technologically well educated.

DI: It is interesting that you referred to the notion of black box. The cultural philosopher and media theorist Vilém Flusser used to reiterate this phrase, in its cybernetic connotation, when talking about the opacity of more advanced technological devices: "The black box is a structurally complex but functionally simple apparatus" (Flusser 1974, 1). Those devices are technologically complex on such a high level that only a few people understand their operating principles. And the rest needs to, or rather wants to, focus on the surfaces of this black boxes, on the interface, engaged by user experience strategies. Do you feel, despite of your work, that many people are not interested in the first place what is actually underneath the surfaces of their devices? That they just want to use their gadgets as easy as possible? How would you approach these people?

DV: It's a really difficult question. In fact, it's a really difficult wall to break through. I don't think there is a working solution to that, really. One of the reasons why this "seamless" technology was created in the first place was to allow those that were not acquainted with technology to start using it: simplification, minimization, graphical user interfaces making it less anxiety-provoking to use computers. All this designated functionality of machines – it's fine as long as their purpose is to allow the user to focus on their task. But what is not fine are the multiple examples where machines are running in the background, tracking your mouse movement or recording your online behavior. There are multiple examples, such as remote Bitcoin farming somewhere that you happen to accidentally load a JavaScript file from.

Currently, I am involved with an NGO, TacticalTech, a collective of about 30 people using computers intensively. Most of my colleagues are pretty good in monitoring and checking out their computers. But even they are sometimes amazed: "My computer is running really hot, I don't know what's going on – I'm not doing things but it's running and blowing." There are really simple ways of checking out what's happening on your computer, what problems it has. But it seems that people aren't even minded that way to go and research how to identify and solve such problems on their own. Which to me is something very alien, because even if my computer is running fine, I still like tinkering with it – and breaking it way too early and way too often [laughs].

Usually, the relationship with technology is, in a way, that it shouldn't be touched. It's so complex that many people don't even start to think about going beyond the interface. Nowadays, more than in the days when I started messing with computers, which was around 20 plus years ago, it is almost a taboo, in a way, for those users that aren't developing anything related to computation directly. It's unadvised, especially by computer manufacturers. There are mechanisms in place, potent and very sophisticated, that prevent what is called tampering with those operating systems, which keep a watchful eye on all the changes that happen to the system running on your computer. In order for the machine to efficiently maintain itself and not to break down it seems that it should not be touched, ever. It was similar back in the '80s: The more expensive cars had their hoods sealed, which you weren't supposed to open, and if you did open it you would risk the warranty. It's an attitude of actually not owning the technology that you are dealing with – rather you are kind of "leasing" that technology. I find that reality so different to what we are actually used to as materialist beings: If you own something, you really, physically own it. But this idea of being leased, a piece of software, or maybe a computer, this feels really wrong.

Many of the efforts that inspired the "Critical Engineering Manifesto" were done in order to break out of this loop; by breaking most of the devices while investigating them you come to realize how the device works. Of course, it requires a particular interest to be willing to do that. And I don't think the manifesto was written in an attempt to make everyone go insane and to break every device they find...

DI: Which would be interesting in its own right!

DV: It would indeed be very interesting! And in fact, it did have such an effect, on a smaller scale [laughs]. It's more about a way of thinking that should be fostered parallel to using a computer: What else happens there? When it is connected to the internet and it uploads and downloads files, is there anything else happening? How is all that regulated?

The further we talk about it, the more there is to add. And I guess that's one of the issues I always have in mind while making my artwork. Most of the pieces are basically illustrations of hacks, computer hacks or sort of unauthorized ways of using one technology or

another. Most of those works were done in an effort to demonstrate what does happen, or what could happen, behind the scenes.

DI: That's actually a very nice transition to another sentence I would like to quote. I believe this one is from the "Critical Engineering Manifesto" and I think it's the strongest one in terms of bringing your mode of work to a point: "The critical engineer considers the exploit to be the most desirable form of exposure" (Oliver, Savičić, and Vasiliev 2011–2019). For me, this is – in one sentence – what you are doing.

DV: Yes, that's a good one. Because how else can you effectively teach someone about what's inside the computer other than by letting the person crack the computer open? The use of the word exploit in this case is very broad. It really depends on your personal aims. What do you want to achieve? If you want to see what's inside of your computer and you open it – yes, you do exploit in a way to gain knowledge about what's inside. And if you want to plant some remote trap somewhere on the internet to intercept someone's data, it's an exploit as well, but with a completely different purpose.

Considering this broad meaning of the word "exploit" I think it can nonetheless be applied very effectively to the educational parts of the hacker movement, for instance. Having taught workshops for the last 15 years to various kinds of people I learned that it's important not to overwhelm those who you try to introduce to ideas of technological domains, but to take it slowly.

DI: Maybe we can talk a bit about the project you are currently working on, which you have titled WannaScry!, obviously a reference to the 2017 WannaCry computer virus. As I understand it, the work will be a critical approach towards video conference systems – a very topical project in times of tackling pandemic-induced social distancing by spending way too much time, at least in my daily routine, in video calls.

DV: As for myself, I always try to avoid video conferences because I find it quite a discomforting experience, I don't know why. I recently went to MediaMarkt[1] and it was sold out of webcams. It reminded me of the early 2000s, when the Web 2.0 was on the rise, how excited

1 Editorial note: A German retail store chain for consumer electronics.

everyone was. But we were forgetting about the fact that the process of content production also produces metadata, and metadata means hundreds of interested third parties. With Web 2.0, for half a decade data communication between Web users defaulted to unprotected protocols, so you could intercept it directly "from the air."

And this is the kind of the situation with video conferencing services today, after the majority of Web users community, or should I say, a major part of human civilization, was forced to use this relatively new video conferencing technology. Not new per se, of course it exists for a long time, but those services have never experienced such a large number of users – who use video-streaming technology not only to consume but to actively generate new, private content. This provoked a wave of interest followed by numerous attempts to intercept and, in a rogue way, participate in private video-calls. It isn't at all unthinkable that state-controlled internet, state-funded internet providers and corporations will be trying to get their hands on this type of information gathering. Because as with private personal metadata back in the days of the Web 2.0, a lot of very private and personal information is nowadays being transferred with video conference software, especially in combination with machine learning algorithms that use your voice, your articulation, your facial expressions – this actually exposes much more of your biometric and personal information compared to any metadata in the days of Web 2.0. For example, by snatching your video call one can train a deep-learning algorithm to recreate a fake identity, which identifies itself with your voice, body movements, facial expressions.

What made me very aware of the fact that those problems are all quite real, was when back in April 2020 a large library of "dumped" Zoom video-calls recordings was found on unprotected Amazon servers. Those dumps were quickly downloaded and re-published by a group of hackers and became known as "Zoom Leaks," and remained available online only for about 5 days, if I recall correctly.[2] There is also a large number of screenshots – pictures of computer screens – with secret IDs for video calls regularly circulating on Twitter, that enable people, like the Dutch journalist Daniel Verlaan

2 Editorial note: A platform for dumped Zoom video call IDs (cf. Krishnan 2020).

in November 2020,[3] to guess access codes and "gate crash" those calls, even when those calls were secret and held by institutions such as the European Ministry of Defence. So, it occurred to me that this environment is a very naive, vulnerable and insecure place.

DI: Thinking about it, the nature of video conferencing – having a pretty good close-up of your facial expressions in combination with a recording of your voice – that's the best dataset for any deep learning algorithm to produce a specific deepfake video.

DV: Yes, absolutely. There are many things to think about and consider when developing such a work, as always. I've been working on WannaScry! since May and the work goes rather slowly, because it's a complex piece. It's supposed to be a physical installation and I already had to work with three different production studios to produce the pieces for it. It takes time, especially in times of COVID-19, having to order something online and until it comes to your studio it takes a month – and then you realize what you had ordered was not the right thing, and you have to order it again; and in the meanwhile, I'm developing the code.

So, since May I've been working on a model of a video conferencing service that is "rigged" to record every conversation that takes place through the service. WannaScry! illustrates a security breach of a video conferencing service and demonstrates the extent to which personal biometric data can be intercepted and extracted by malicious cyber agents seeking to create and puppeteer alternate identities, potentially with the aid of machine learning algorithms. With this project I want to draw attention to the next generation of human-machine interrelationships and vulnerabilities. Familiarizing oneself with the benefits and hazards intrinsic to the use of digital tools and networking technology is necessary in order to safely navigate the internet and secure one's cyber-wellbeing. To make an informed choice of digital tools, including those for protecting our digital rights, one would first need to understand what compromises are involved by

3 Editorial note: In November 2020, the Dutch journalist Daniel Verlaan accessed a Zoom meeting of EU defence ministers after guessing the access code pattern visible in photo posted on Twitter by the Dutch defence minister Ank Bijleveld (Deutsche Welle 2020).

engaging with the latest technological trends. This includes, especially during the current pandemic crisis and its digitally aided social distancing, video conference systems.

Thinking about this complex in an exhibition context, video and audio data, plus some of the video call-specific meta information about the persons participating in the call will be displayed. The plan is to make WannaScry! interactive: Visitors can use their mobile device to make a video call using the service by inviting someone from the audience and/or someone online to watch their conversation displayed as it's captured in real-time and projected onto the WannaScry! sphere. All the while this will be rendered into a form of a scrying ball, a "palantír"-like device, like the all-seeing stone in Tolkien's *The Lord of the Rings* – a device remotely connected to a person, ready to tell you about their deepest secrets and insecurities.

My interest, however, is not to sneak up and hear peoples' secrets, but rather to have those very people be confronted by my work, to see themselves revealed by a seemingly innocuous "gazing ball" and realize that, whenever you talk to your computer, you're not talking to your intimate partner alone – you are actually talking to everyone who wants to listen and has the capability to do so.

DI: When you decided to give the work a form resembling a "palantír," are you also, subtly, pointing to Peter Thiel's surveillance corporation with the same name?

DV: Well, I originally didn't think about a palantír, the seeing stone, but it happens to be the culturally most known reference for such a device. I was thinking about gazing into a misty scrying ball with "supernatural" capabilities. One of the established terms in the paranormal domain is "remote viewing" – an extrasensory ability to connect to and to read remote minds... An ability which nowadays internet services can facilitate quite well, thinking of the internet as a rhizome network that we all are a part of – a parallel dimension of sorts where one can plant a probe in and suck all the information out. This is when the Palantir Technologies company reference comes into play and contributes a terrifying example of how real all this is.

The machine that I'm building aims to lure people into using it, while at the same time it's not an attempt to scam people – it is going to be in an exhibition with a big sign on it saying, "connect to this

URL and see your private conversation being made public." It's about making explicit the exploit of this technology in an attempt to help people understand the potential of such an exploit as a result of their own personal choices.

DI: Is it going to be connected to video-conference service of a bigger provider or will it run on your own platform?

DV: It's my own platform, and people will know that it isn't a real provider. I'm not going to try to be as promiscuous as one would need to be in order to pretend being a real provider.

Another aspect, a parallel thought which touches less on media theory or cultural impact of technology, but which is rather about the techno-political aspect of open source, is the fact that the software I'm using to create this rigged service is open source software. This means that anyone could make exactly the same modifications as I did, to create such a palantír and plant it somewhere online. Then advertise their platform as a completely legitimate, free-to-use service while covertly retaining your data. The thing about safety and security that open source software promises, is that since the software base is entirely open, it does not prevent anyone to come in and make modifications that might not be beneficial for the users of that software or technology. It's one thing to be running open source software on your laptop – you installed it and there was no third party involved – but it is an entirely different story when open source software is used as an online service. Just the fact of connecting to servers that claim to be running open source software doesn't mean that this open source software wasn't modified in some way. On an industrial level, there are ways to verify the validity and coherency of such software installed on a server – package checksums, automated auditing, etc. – but such practices have never reached the consumer market, or rather consumer-facing substrate of the market. When you connect to some random server, one assumes – or chooses to believe – that the server's software doesn't contain any sinister modifications. But if modifications did in fact occur there is no mechanism in place that would notify the user about these modifications, there is no security check between a user and a web service based on open source software. It is for that very virtue that the trust we put in a service running on top of open source software relies solely on the reputation

of those who run the service and not the software itself – which is in fact a concerning issue.

DI: Do you know how you will form or design the aesthetic aspect of your work? How will you present it to make it expose its functions, or intentions, so to speak?

DV: Well, this is still in flux. I want to have it look and feel as close as possible to an ordinary, everyday experience of using video conferencing services. But, of course, given the fact that it will be shown in an exhibition context with people around it, for that reason I'm creating this palantír-like device, a sphere on which recordings of video-calls and personal information is going to be projected. There is a potential for the work to be interactive, so you could actually scroll through and watch video calls and listen to conversations which have taken place. The main intention is to make sure that, whoever approaches the work, they come to realize that whatever passes through such a system can be captured, exposed – and exploited.

DI: Do you plan an extension of the work that shows possible results of such an exploit, say, a deepfake application of the data harvested?

DV: That would be a far-reaching extension, because most of the analysis needed for teaching an algorithm isn't done in real-time. So, it might be like a chapter 2 of the work, as in "and here we can see what the machine has learned" [laughs]. In the current context, I see the device more as signifying a source of gathered information which could potentially be passed on to either black markets or third-party buyers, for instance data-brokers, who illicitly acquire private personal information. This is why, for now, I'm going to focus on *how* information is gathered, rather than what happens next.

There are so many aspects to consider in a project like WannaScry!, so I first need to work on what I can realize and then take it further. That's the thing, you see, about artworks created in this field – you cannot treat them as a product, you cannot treat them as a service. Because once you start doing that you will end up in this loop of maintenance, servicing and user support. It has to be bound by time. Artworks are created to illustrate the contemporary state, as in the current state of time when the artwork was created.

I wouldn't want to maintain an artwork to make it function for the next ten years because that's not the point. By the time I finish the work, it might already be obsolete and possibly dysfunctional. "Newstweek," for example, a project on which Julian and I worked in 2011, signified the extreme openness of unencrypted, clear-text network communication.[4] A year after we had released Newstweek, Edward Snowden came out with his NSA revelations and everything on the Web became encrypted using HTTPS/TLS. Which was great – and instantly made Newstweek be a thing of the past.

DI: So, your work has a "best before – things get better" date.

DV: Yes, "expired before released!"

DI: You mentioned data-brokers, we talked about deepfake. What issues can you imagine – intended and maybe unintended ones – that your work will address or discussions it will trigger once it is running and will be exhibited?

DV: So far, I've been – ambitiously! – thinking about creating a profile for each person, for instance a voice signature; a biometric signature, such as the face; place of origin, or at least place of origin of the call. And I was thinking about creating some kind of dataset of the conversations that people conduct through the system. But since there isn't really a selection for any particular subject that will be discussed, it will be rather about demonstrating the potential functionality of such a system in place.

Here is an example: if a proxy, a *man-in-the-middle* server, capable of retaining video call information is placed in an office of a political party, then you could search for much more specific data in those conversations, and maybe employ something like a speech-to-text conversion to create machine-readable pieces of conversations that took place – for instance. I don't think about WannaScry! as a project on stealing any particular type of data, rather the work is there to spark attention of the public about these weaknesses, about

4 Editorial note: "Newstweek" (2011) is based on devices that can alter the content of news websites read on public wireless networks. It was developed in collaboration with Julian Oliver and received the Ars Electronica Golden Nica award in 2011.

vulnerability, about the possibility of security and privacy breaches happening – and again, again and again saying that whenever you converse using your computer and the internet, you are not conducting an intimate, private conversation.

DI: Here we could come back to Vilém Flusser. He died in 1991, so before the rise of the World Wide Web. But he wrote about the coming "telematic society" because at the time, from 1972 on, he lived in France, where the Minitel, the French national "proto-internet" was rolled out in the 1980s. The possibility to communicate via networked computers he sometimes described as "telepresence," a term also popular with artists at the time and during the course of the 1990s: to interact with the other over longer distances, implying that time and space is vanishing – this old McLuhanism, a utopian concept. Online video conferences are actually the perfect vehicle for this narrative, a quite romantic narrative.

But now your work is turning this on its head: Especially in times of social distancing, one wants to be closer to the distant other. One wants to have an intimate conversation – but just that it's not. The whole purpose of the exploit you are addressing is to collect data, observe behavior. Maybe it is a too general question, but would you agree that your whole body of work is about going against this utopian concept of McLuhanism, or of Flusser, for that matter – the promises of computer networks to intersubjectively connect free individuals?

DV: The frightening and at the same time interesting part for me is that the exploit is inevitable. Even if it creeps you out, you are part of it. I think it could have been a different story before the early 2000s, before people figured out that there is a lot of money in this business, that it was doomed to become a money-making machine harvesting data. It's a very symbiotic relationship between business and technology, obviously a lot of money is been poured into internet technology in general and, because of that the market, has become a hyper-production.

And that's what we are facing now – it's like a black hole, it had to suck everything in, in order to become ever more efficient in making money and generating return on investment for venture capitalists. That's the sad truth. The fact that technology has become more integrated into our lives and at the same time harder to learn, I think

that is just an unfortunate side effect of this "evolution." Practically any modification one would want to apply to current computer and networking technology would require a lot of knowledge of hardware, software and of computer science.

Honestly, I really miss the days of the late 80s and 90s, when technology was wide open. If I was to grow up today, I probably would have a very hard time finding entry points. If you try to educate children today about technology based on this multi-layered stack of abstractions that we now have... It oversimplifies technology to an extend that it actually removes it. There's a statement by Steve Jobs, or maybe someone else at Apple, from around 2010 about the design of the iPad:[5] Their goal was to remove the feeling of being confronted with anything, to achieve this seamlessness, this sort of intuitiveness – which is good, definitely, I'm all for technology being intuitive. Already with the desktop metaphor, if one wants to go back as far as that: We always attempt to confront the user with the least. But if you consider the current state of things today – this might have been the wrong move. Because while it allows more people to start using computers, a lot of knowledge has been lost or hasn't been recovered. I think this is something that we are missing these days, that we are lacking. There is a growing divide between our technological advance and our information literacy.

One symptom of that is the difficulties of having to separate truth from falsehood, to simply be aware of the fact that what is displayed on a screen of your device is not necessarily what you would want to believe. But that had become a standard, an assumption, to an extent, turning into a quasi-religious belief. Because we are all told that the computer is right, that data gets results right. And this is something I wish we could change. It is difficult to discuss my work and the work of my colleagues without going into deeper, darker details. That's one of the major challenges I face in general when talking about my own work, mainly because there is a huge techno-political aspect to it. Also, there is a necessary aesthetic dimension, the ways of presenting the work and having to bring that all together so that

5 Editorial note: In an ad for the Apple iPad in 2012 the narrator claims: "We believe that technology is at its very best when it is invisible." Cf. a video montage by the web artist Olia Lialina juxtaposing this ad with a video statement by Marshall McLuhan conducting a warning of technology's "irresistible force when invisible": https://www.youtube.com/watch?v=9gx-zHHItQs&feature=youtu.be.

it actually works for different kinds of people: for those who come to look at it as a technological exploit, for those who see it as a cultural manifestation, or for those who receive it as a political message – those three components are definitely at play, always.

DI: You mentioned the iPad and the desktop metaphor...

DV: Such an old school thing!

DI: Yes, but still relevant. It made me think about Alan Kay and his team at Xerox PARC in the 1970s who came up with the desktop metaphor. Kay focusing on user experience, including the graphical user interface, also came up with a very early – maybe the first – tablet computer concept, the "Dynabook" (Kay 1972). And this is interesting, because he had the idea that the Dynabook should be an openly accessible computer for basically everyone – in fact that accessible that children would be able to use it. Children should be able to work with it, not only on a superficial level but also on a level that enabled them to learn how to code. The Dynabook wasn't functional, though, it was a mock-up, a thought experiment. Later, Kay and his team would go on to develop the object-oriented programming language Smalltalk as a new way of computing – a "human-computer symbiosis."

DV: But the problem with these things, as well as with interactive media art, for instance, is the sense of: Why? Why would a child come to a computer and try to program it? And "why?" not in a rejectionist way but as in: What would make a child, or anyone for that matter, do something with the computer that is new or not in the user manual?

DI: And not directly rewarding.

DV: Yes. How do you make people start to experiment with computers?

DI: Maybe it's because the Dynabook concept was conceived by Alan Kay, who was himself a tinkerer, who probably got the Altair when it came out and who would take an inherent pleasure in tinkering for granted.

DV: Sure, it's taken for granted, and this is very often a struggle in the open source world as well: People make software for likes of their own. For instance, how user interfaces for open source software are often unusable, because it's the last thing that has been thought of.

Someone told me that artists are like interpreters. Even back in history, an artist would create an image that would manifest an event or time period for others to look at and enjoy the beauty of the landscape, but also to learn about the time that it had been made in, even if unintentionally. By having to be that interpreter, artists actually try to explain something that they think might be misunderstood. And that maybe helps to motivate people to start questioning cultural or technological artifacts as well – and to conduct their own experiments.

DI: A good call for a good closing sentence! Thank you, Danja, for your time.

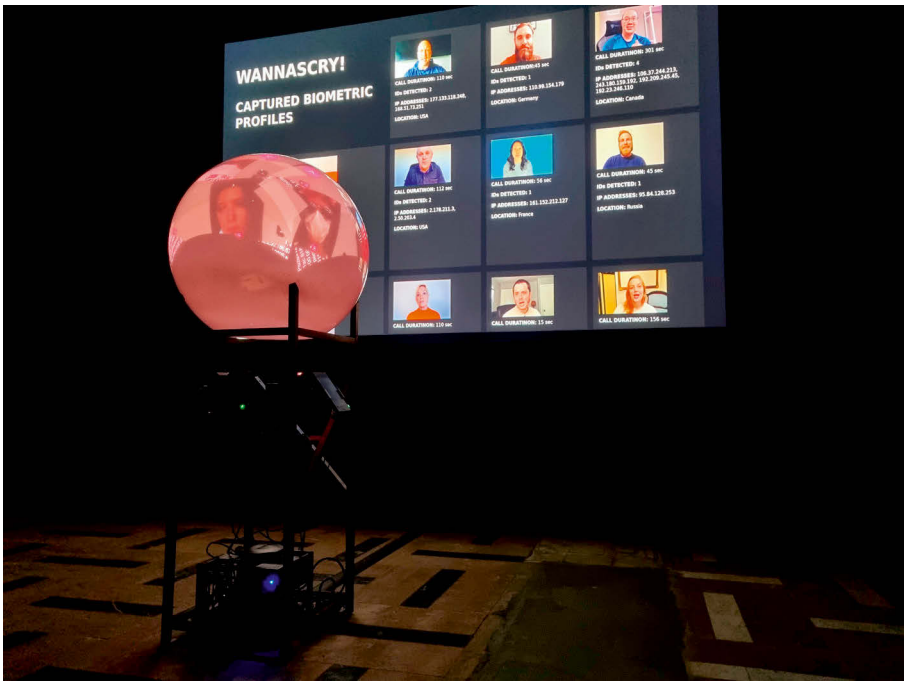

Fig. 1 Danja Vasiliev: WannaScry! at Laboratoria Art&Science exhibition, Moscow (June 2021).

References

Deutsche Welle. 2020. "Dutch reporter hacks EU defense ministers' meeting." *Deutsche Welle*, November 20, 2020. https://www.dw.com/en/dutch-reporter-hacks-eu-defense-ministers-meeting/a-55682752.

Flusser, Vilém. 1974. *Two Approaches to the Phenomenon "Television"*. Manuscript Vilém Flusser Archive, ref. no. 3110.

Kay, Alan. 1972. "A Personal Computer for Children of All Ages." Xerox Palo Alto Research Center. https://www.mprove.de/visionreality/media/kay72.html.

Krishnan, Rakesh. 2020. "ZOOM LEAKS – A Platform for finding leaked Meetings." *Medium.com*, April 2, 2020. https://rakeshkrish.medium.com/zoom-leaks-a-platform-for-finding-leaked-meetings-89b962b9ac2e.

Oliver, Julian, and Danja Vasilev. 2016. "Quarantined." In *across & beyond – A transmediale Reader on Post-digital Practices, Concepts, and Institutions*, edited by Ryan Bishop, Kristoffer Gansing, Jussi Parikka and Elvia Wilk, 198–201. Berlin: Sternberg Press.

Oliver, Julian, Gordan Savičić, and Danja Vasiliev. 2011–2019. "The Critical Engineering Manifesto". https://criticalengineering.org/en.