



CRITICAL ENGINEERING

Radical Tools for Interventions in Infrastructure

Tactics&Practice #7

1

CRITICAL ENGINEERING

Radical Tools for Interventions in Infrastructure

TALKS | WORKSHOP | EXHIBITION

Ljubljana, 26–27 March 2019

INTRODUCTION	2
PROGRAMME OVERVIEW and REGISTRATION	3
THE TALKS	4
THE WORKSHOP	7
THE EXHIBITION	8
BIOGRAPHIES OF THE PARTICIPANTS	10
CREDITS and CONTACT	12

INTRODUCTION

In 2011, a group of artists and engineers published the [“Critical Engineering Manifesto”](#), since translated into 18 languages. Around the manifesto, originally written by Julian Oliver, Gordan Savičić and Danja Vasiliev, gathered a larger group – the Critical Engineering Working Group – now including also Sarah Grant, Bengt Sjöln and Joana Moll.

In true avant-garde fashion, the “Manifesto” launches by describing Engineering as “the most transformative language of our time, shaping the way we move, communicate and think”, thus, it is the work of the Critical Engineer “to study and exploit this language, exposing its influence”. Further, a Critical Engineer “recognises that each work of engineering engineers its user”, considering “any technology depended upon to be both a challenge and a threat”. And so the manifesto unfolds.

Nearly ten years later, the relevance of the “Critical Engineering Manifesto” has only become more evident, as an ever-growing public becomes aware of the techno-political implications of using – and depending upon – integrated systems and complex, networked technologies. Today, one can find its 11 points listed on the walls of hacklabs, museums, engineering and media-art academies, and in a great many texts, the world over.

The *Tactics&Practice* event entitled *Critical Engineering* comprises an exhibition, a seminar and a workshop, underlining the artistic, theoretical and educational work done by the Critical Engineering Working Group along the last decade. The seminar will host all the members of the group – all of them recognised artists with long individual artistic careers – using their statements and their projects as case studies to analyse the transformative potential of Critical Engineering in the context of a tactical and technical arts practice.

PROGRAMME OVERVIEW

THE TALKS:

 [Kino Šiška](#), Trg prekomorskih brigad 3, Ljubljana
Tuesday, 26 March 2019

17:00 Julian Oliver & Danja Vasiliev: *Dark Internet Topologies*
17:45 Gordan Savičić & Bengt Sjöln: *Electromagnetic Situationism*
18:30 Joana Moll: *An Autopsy of Data Business*
19:15 Sarah Grant: *Radical Networks*

THE WORKSHOP:

 [Kino Šiška](#), Trg prekomorskih brigad 3, Ljubljana
Wednesday, 27 March 2019

09:00–18:00 Sarah Grant & Joana Moll: *Surveillance Override*

EXHIBITION:

 [Aksioma | Project Space](#), Komenskega 18, Ljubljana
Wednesday, 27 March 2019

19:00 *Critical Engineering* (opening)

Open through 26 April 2019

REGISTRATION

[Please fill in the registration form by 24 March 2019](#)

The conference will be held in English. Free admission.

THE TALKS

 [Kino Šiška](#), Trg prekomorskih brigad 3, Ljubljana
Tuesday, 26 March 2019, 17:00–20:00

In an evening of 4 talks by 6 speakers, we'll hear from the Critical Engineering Working Group members about their work together as well as outside the group. Tracing territories from the dark topologies of the internet to the factories and apparatus beyond the interface of our electronic devices, our guest speakers will question what interconnectivity and public space might truly look like in today's so-called networked age.

Julian Oliver & Danja Vasiliev

Dark Internet Topologies



In this talk, Julian Oliver and Danja Vasiliev will give an overview of “dark internet topologies” in the context of their commissioned piece *Vending Private Network*. Challenging the popular reading of the internet as a digital incarnation of the commons, “public space”, they will – using command line utilities known to network administrators – reveal a deep and original privatisation, one that necessitates new “dark abstractions” to achieve the public space we expect from it. In doing so, they show how “darknets” are technical implementations of the same rights structures we value and actively defend within corporeal public life.

Gordan Savičić & Bengt Sjölén

Electromagnetic Situationism



Gordan Savičić and Bengt Sjölén will talk about works developed together with the Critical Engineering Working Group. Both artists explore network situations in which the electromagnetic infrastructure has been used as a field of intervention. Making use of contemporary technologies such as software-defined radio, they examine the analysis and reconstruction of any leaked signal over the air, independent of whether it originated from an intentional transmission at an antenna or from an unintentional emanation from a conductor on a substrate. The electromagnetic space serves as research framework for developing investigations into the traces and shadows of our technological dependency.

5

Joana Moll

An Autopsy of Data Business



Our so-called networked society has failed so far to transpose the logic of interconnectedness into our lives. Citizens are becoming increasingly machine-like and dependent on data, threatening the connection between humans and their natural habitats. Although most of our

daily transactions are carried out through electronic devices, we know very little of the apparatus that facilitates such interactions, or in other words, about the factory that lies beyond the interface.

Sarah Grant

Radical Networks



Radical Networks is an international conference and arts festival which features practitioners working with the electromagnetic spectrum in critical and creative ways. In response to the obfuscation of the inner workings and issues that arise from being an always-on, internetworked society, Radical Networks seeks to demystify and push those very things to the foreground of our consciousness. Sarah Grant will discuss some of the thinking that has led to the creation of Radical Networks as well as what it hopes to achieve as a community focused event, including highlights from past talks.

THE WORKSHOP

Sarah Grant & Joana Moll

Surveillance Override

 [Kino Šiška](#), Trg prekomorskih brigad 3, Ljubljana
Wednesday, 27 March 2019, 09:00–18:00

Limited to 12 participants

FREE OF CHARGE. APPLICATION MANDATORY

Participants will be selected based on a short motivational letter. Follow [THIS LINK](#) to apply and tell us WHY you think you will benefit from it.

DEADLINE FOR SUBMISSION: 20 March 2019, midnight

Psychological Warfare, also called PSYOPS, is a strategy used in military and government intelligence networks aimed at influencing the emotional, cognitive and rational structures of governments, organisations, groups, and individuals, in order to change their behaviours and ultimately their purposes and goals. PSYOPS tactics are deeply rooted in the diverse techno-social arrangements that lie at the core of algorithmic governance, yet they are often ignored or overlooked by most global citizens, who nevertheless operate within such arrangements. With increasing distrust in “The Cloud” comes a broad call for publicly-owned network infrastructures that would give users greater control over their personal communication, data and identities.

In this 8-hour, hands-on workshop we will try to connect the dots between PSYOPS, psychology, propaganda, surveillance, the internet, data and algorithms, and we will underline the need to build alternative networks to retain sovereignty over our communications technologies and natural resources.

In the first part of the workshop, Joana Moll will give participants a deep understanding about the many mechanisms used by corporations, agencies and governments to collect, sort and exploit personal data, along with the main social, political and environmental impacts of such processes. In the second part, Sarah Grant will introduce participants to the basic building blocks of computer networking, command line interface and WiFi communication. We will learn how to self-host our own web servers, file servers and personal wireless networks. These servers will allow their users to send messages, publish websites and share files across an offline local area and mesh network.

THE EXHIBITION

Critical Engineering Working Group

Critical Engineering

 [Aksioma | Project Space](#), Komenskega 18, Ljubljana
27 March–26 April 2019

Exhibition opening: WED, 27 March 2019, 19:00

Opening hours: TUE–FRI, 12:00–18:00

How can we use engineering to visualise, respond to and resist the daily, strenuous – and mostly successful – effort perpetrated by the tools and infrastructures designed by corporate and governmental subjects to engineer us? Intended as “radical tools for interventions in infrastructure”, the works developed by the Critical Engineering Working Group offer different answers to this question, from simplified, easy access to resistance tools, to hijacking technological infrastructures in order to expose their inner workings.

According to the *Critical Engineering Manifesto*, “the greater the dependence on a technology the greater the need to study and expose its inner workings, regardless of ownership or legal provision”. Thus, it’s no surprise that the three “tools for intervention” presented in this exhibition focus on networked infrastructures and online communication, especially WiFi communication via portable devices: technologies we depend upon to communicate as well as to locate ourselves in the physical space, yet that are also used to control and follow us.

8

EXHIBITED WORKS

Julian Oliver, Danja Vasiliev

Vending Private Network, 2018

Vending Private Network takes the form of a condom-vending machine, such as those typically seen in public toilets, nightclubs and bars. Equipped with mechanical buttons, a coin-slot and USB ports, it offers 4 VPN routes, each with an animated graphic depicting the route as a fantasy destination. Visitors are invited to insert a USB stick into the slot, a coin (1 pound or euro) into the machine, and to select a VPN destination by pressing a mechanical button. In doing so, a unique VPN configuration file is then written to the USB stick. Special instructions (in the form of a README.txt) are also copied, explaining how to use the VPN in a special “sheathed” mode that evades detection methods (namely Deep Packet Inspection, or DPI) used by corporations and state-controlled infrastructure administrators. This is the only means known to work against state-controlled firewalls.

Bengt Sjöln, Gordan Savičić

Packetbrücke, 2012

Packetbrücke (*Packetbridge*) explores the simulation of entire network situations by transferring the electromagnetic infrastructure to a different physical space. The result is a revealing “confusion” of devices and services reliant on this infrastructure. Wireless network packets are directly captured from a specific location and tunnelled through the internet to a remote location, where they are released back into the air. In doing so, *Packetbridge* literally injects one electromagnetic representation of geographical space into another, effectively producing a new imaginary topography and, through this remediation, an “impossible reality”. *Packetbridge* demonstrates that positioning systems based on WLAN are a site for intervention, at the same time expressing their vulnerability to location spoofing attacks.

Bengt Sjöln, Danja Vasiliev

Unintended Emissions, 2015

Inserted into urban environs, *Unintended Emissions* captures, dissects, maps and projects radio emissions unintentionally and invisibly shared by our portable wireless devices. Employing two arrays of directional Yagi antennas, the project attempts to determine positions of WiFi devices in the vicinity. Similarly to surveillance and tracking systems such as StingRay, *Unintended Emissions* places mobile WiFi users on to a map indicating the kind of a device a user has, the time of appearance, the user’s network activity and other user-specific metadata. This information can be further analysed to determine the user’s identity and movements within a locality and the internet. Using methods and technologies known to be deployed by federal surveillance initiatives, the intervention seeks to engender a “healthy paranoia” in the interests of an increased techno-political subjectivity.

BIOGRAPHIES OF THE PARTICIPANTS

Sarah Grant is an American media artist and educator, currently based in Berlin. Her areas of focus are bio-circuitry, sculpture, radio and computer networks. She has taught workshops on self-hosting and DIY networks around the world. She is a former research fellow at the Tow Center for Journalism at Columbia, adjunct professor at NYU Polytechnic in Digital Media, and resident at the Eyebeam Art and Technology Center. Additionally, she is the author of *Subnodes* and organises *Radical Networks*, a community conference and arts festival for creative, critical and alternative applications of internet technology.

Joana Moll is a Barcelona/Berlin based artist and researcher. Her work critically explores the way post-capitalist narratives affect the alphabetisation of machines, humans and ecosystems. Her main research topics include internet materiality, surveillance, social profiling and interfaces. She has lectured, performed and exhibited her work in different museums, art centres, universities, festivals and publications around the world. She is the co-founder of the Critical Interface Politics Research Group at HANGAR (Barcelona) as well as the Institute for the Advancement of Popular Automatism. She is currently a visiting lecturer at Universität Potsdam and Escola Superior d'Art de Vic (Barcelona).

Julian Oliver is a New Zealander, Critical Engineer and artist based in Berlin. His work and lectures have been presented at many museums, galleries, international electronic-art events and conferences, including Tate Modern, Ars Electronica, transmediale and the Japan Media Arts Festival. He has received several awards, most notably the distinguished *Golden Nica* at Prix Ars Electronica 2011 for the project *Newstweek* (with Danja Vasiliev). He is the co-author of the *Critical Engineering Manifesto* and co-founder of *Crypto Party* in Berlin. Julian has given numerous workshops and master classes in software art, data forensics, creative hacking, computer networking, counter-surveillance, object-oriented programming for artists, augmented reality, virtual architecture, video-game development, information visualisation and UNIX/Linux worldwide. Articles about his work have appeared in the *New York Times*, the *Guardian*, *Wired*, *Der Spiegel*, *El Pais* and *Liberation*, among others, and on several TV channels worldwide including the BBC.

Gordan Savičić, born in Vienna, is a Swiss-based artist and designer whose work investigates the relationship between people, networks and interfaces. He has a background in media art and visual communication and has been active within the fields of academic research, teaching and the design industry. Savičić holds a BA in Digital Art and New Media from the University of Applied Arts Vienna and an MA from the Piet Zwart Institute in Rotterdam. His participation in collaborative projects and performances have been shown in several countries and received various awards, such as Japan (dis-locate), Germany (transmediale), Austria (Ars Electronica) and Spain (Arco), among others.

Based in Stockholm and Berlin, **Bengt Sjöln** is an independent software and hardware designer, hacker and artist with roots in the home computer demo scene. He collaborates with

several networks, including Weise7 in Berlin, Teenage Engineering in Stockholm, and aether architecture in Budapest. His current and continuous experimentation spans the programmatic generation of design, function, hardware and code, electromagnetic investigations, networking technologies, reverse engineering, molecular life science, architecture, visualisations and visuals, sound and self-modifying code.

Danja Vasiliev is a Berlin-based, Russian artist and Critical Engineer. He studies systems and networks through anti-disciplinary experimentation with hardware, firmware and software. Using computational platforms, he engages in the examination and exploitation of system and network paradigms in both the physical and digital realms. Based on these findings, he creates and exhibits works of Critical Engineering. Since 1999, Vasiliev has been involved in computer-technology events, media-art exhibitions and seminars around the world. He has received several awards and mentions at Ars Electronica, Japan Media Art Festival and transmediale, among others. In October 2011, together with Julian Oliver and Gordan Savičić, he co-authored the “Critical Engineering Manifesto”. He gives public workshops and talks as well as regularly teaches courses on network insecurity, software/OS modification, hardware re-engineering, digital forensics and other technology related subjects.

CREDITS

Tactics&Practice #7 -- Critical Engineering

Curated by: the Critical Engineering Working Group

Artistic director: Janez Janša

Head of production: Marcela Okretič

Executive producer: Sonja Grdina

Development Specialist: Jana Renéé Wilcoxon

Technician: Valter Udovičič

Public relations: Urška Barut

Documentation: Miha Fras (photo), Gregor Gobec (video)

Corporate visual identity: Luka Umek

PRODUCTION: Aksioma – Institute for Contemporary Art, Ljubljana, 2019



COPRODUCTION: Kino Šiška Centre for Urban Culture, Ljubljana and Drugo more, Rijeka

12



Critical Engineering is realised in the framework of [State Machines](#), a joint project by [Aksioma](#) (SI), [Drugo more](#) (HR), [Furtherfield](#) (UK), [Institute of Network Cultures](#) (NL) and [NeMe](#) (CY).

STATE MACHINES

SUPPORTED BY: the Creative Europe programme of the European Union, the Ministry of Culture of the Republic of Slovenia, the Municipality of Ljubljana.



MEDIA SPONSOR: Radio Študent and TAM-TAM



TAM TAM

This project has been funded with support from the European Commission. This communication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CONTACT

[Aksioma | Institute for Contemporary Art, Ljubljana](#)