Anna Engelhardt
Insurgent Computing

Shintaro Miyazaki: So how would you describe or define insurgent computing?

Anna Engelhardt: Insurgency is a military term usually used by the imperial powers as a synonym for rebellion or struggle, amplifying its unlawful and violent nature. Such a definition is not enough, though, to explain the concept of insurgent computing, I propose. What is important is the context in which U.S. military scholars developed such a definition—the context of counterinsurgency operations, i.e. colonial wars fought since the ’70s until the new era of counterterrorism was established in the 2000s. This understanding of insurgency, which is essentially very similar to guerilla fighting, bears the critical aspects of decolonial resistance, such as its main advantage: asymmetry between information and communication. In the colonial wars, what I call the Empire (the Soviet and later Russian state) has always felt lost trying to locate the enemy, as the entire environment is hostile towards data extraction: locals do their best not to disclose information to colonial invaders, maps of the territory are lacking or outdated, routes for communication are scarce and less developed than those operated by decolonial resistance, etc. I propose to take such asymmetry of information and communication as the core of insurgent computing.

In fact, not only do I suggest doing so, but this understanding, though formulated differently, was at the core of the notion of cyberwar in the ’90s. As the central cyberwar thinkers of the RAND Corporation proposed, information, revolution, and the rise of networks exacerbated the already existing threat of highly coordinated insurgencies. They show such potential of insurgent computing in the book *The Zapatista’ Social Netwar’ in Mexico* (1999) or chapters like “The Networking of Terror in the Information Age” in *Networks and Netwars* (2001). In the same year, in 2001, the second issue of the journal *Tiqqun* came out, with the article “L’hypothèse cybernétique.” “The Cybernetic Hypothesis” is arguably one of the most well-known texts of this generation of thought, which argues for the cybernetic diffusion of guerrilla war, invisible to the eyes of the Empire. It is essential for insurgent computing, as it analyses the role information and its withdrawal could play in such an organisation.

Shintaro Miyazaki: Thanks. Now I have a better grasp of insurgent computing. You mentioned “colonial wars.” What kind of wars do you mean concretely?

Anna Engelhardt: In my research and practice, I deal with colonial wars fought by the Soviet and, later, the Russian state. Those are Soviet military intervention in Afghanistan (1979–1989), Russia’s first (1994–1996) and second (1999–2009) invasions of Chechnya, the occupation of Ukrainian territories (2014–present), and war in Syria (2015– present). Information and communication asymmetry has been the primary cause of losses among Russian soldiers in all of these wars, from the friendly fire intentionally staged by the resistance to ambush attacks.

According to Antoine Bousquet, this has also been the case with the U.S. campaigns. In his book on scientific modes of military fighting, he describes the failure of American cybernetic warfare in Vietnam, where “the world’s most powerful and technologically advanced military was unable to overcome a Third World guerrilla army” (Bousquet, 2009). Bousquet analysed how U.S. officials, faced with the information asymmetry of guerilla fighting, only exacerbated such asymmetry. Obsessed with the quantities of collected information rather than its quality, the Pentagon drove itself deeper into “the fog of war.” These failures bring out evident parallels with contemporary drone warfare, which forces their operators to “drown in data” from the multitude of sensors (Graham, 2016).

Shintaro Miyazaki: Earlier, you rather described what you mean by insurgency. So let me ask again a bit different: How is insurgent computing different from insurgency? What does the computing component bring to such a term?

Anna Engelhardt: Insurgent computing can create novel networks or sabotage existing ones. For instance, the app March (Марш, from Russian ‘Demo’), developed in Belarus in autumn of 2020, allowed protesters to communicate with each other in an environment of governmental interference into mobile data. With no functional internet connection, protesters in Minsk could still keep the app online through SMS or Bluetooth, updating each other about water cannons, mass arrests, undercover police, special forces, location of the mass demonstrations, etc. Similar apps were recently developed in Hong Kong, warning users if they were heading towards an area actively patrolled by police. These two instances illustrate well how computing in insurgency allows users to remain updated and invisible by amplifying the information and communication asymmetry.

To explain the conceptual grounds of “computing” in “insurgent computing,” I would like to recall the “cyber” of “cyberattack,” as I imagine these terms to be similar. The “cyber” in “cyberattack” refers to networks. When these networks are attacked digitally, they are called computer or information networks. If the damage of a cyberattack is analogue—like the electricity blackout caused by the Russian forces in Ukraine in 2015—these networks are called infrastructures. Therefore, cyber is something more inclusive than simply the “internet,” simultaneously positioned in both digital and analogue domains. “Computing” in “insurgent computing” should also be understood with a network at its core, an information-rich network, to be precise. The difference would come from the active agency implied in the term—rather than an environment (cyber) where something takes place, it refers to a performed action (computing). Computing, according to such an understanding, aligns well with conventional practices of insurgency, such as sabotage of transport networks. Indeed, computing builds upon the close relationship between insurgencies and networks. It highlights the information as an operational quality of such a network. One can successfully blockade a railroad or a pipeline like the Wet’suwet’en people did. But one could also help such resistance or initiate one’s own resistance action remotely by rendering the Coastal GasLink Pipeline dysfunctional through denial-of-service or supply chain attacks, or else on the ground through spoofing, wiretapping, fibre tapping, etc.

Shintaro Miyazaki: How do you engage with insurgent computing in your practice and theoretical work?

Anna Engelhardt: As an artist, I aim to create or imagine digital environments that exacerbate information asymmetry, create and sabotage networks. In our project Intra-structures, developed with my collaborator Sasha Shestakova and coded by eeefff, we analysed the back-end of Russian propaganda production. We conceived the project as a fictioning machine, practically realised as a Telegram bot (its handle on Telegram is @intr4_bot). Over the course of a week, the bot provides subscribers with the mundane chat of propaganda workers, discussing complications of doctoring satellite images, PR managers’ phones losing signal, drones photographing tarps on the ground.

My most recent work, Circuits of Truth, has been evolving throughout the last year. Drawing on the notion of hardware interfaces, it reframes blue verification ticks as an information processing device whose function is to encode and decode signals. The project looks into the circuits of this device, showing how polarisation between ‘true’ and ‘fake’ is manufactured. Dissecting various forms of authenticity is also a personal concern, as someone who has to operate under an alias due to the political content of my work. Speaking to thinkers and practitioners of digital conflict in Circuits of Truth helps me situate myself in the cyberwar landscape and search for the prospects of my practice within this context. One of those possibilities comes from my collaboration with Medina Bazargali, with whom I have developed my digital face that I use for all online public appearances.

As a thinker, the way I engage with insurgent computing comes as an intersection of two lines of thought that have been enormously influential for me. Reduced to personalities, they can be represented by

Svitlana Matviyenko and Laleh Khalili. Svitlana Matviyenko is a cyberwar thinker who, as an expert in Lacanian psychoanalysis, dissects identity and class struggle in digital conflict with a unique depth. Laleh Khalili has, over the years, developed the whole body of work on colonial practices employed by the U.S., with her work on U.S. counterinsurgencies central for my research. I seek to establish through my thinking the notion of digital colonialism and decolonisation—not as a metaphor but as an actual practice of contemporary colonial regimes that weaponise information networks and those who resist them. I feel there is a turn in decolonial thinking which is about to happen, a turn that would welcome the issues of digital terrains, blockades, infrastructure to be situated close to the material ones. So far, colonialism on digital terrains has been reduced to physical infrastructures that enable those spaces. Colonial violence has been successfully called out, but only on the very land the decolonial struggle is used to. What could be gained from strategies of resistance that could be simultaneously digital and analogue? I feel this is what I already see in Seb Franklin’s book *The Digitally Disposed: Racial Capitalism and the Informatics of Value* published earlier this year. In his work, Franklin successfully dissects digitality as a simultaneously material and immaterial phenomenon, making an outstanding analysis of dispossession and expropriation.

Shintaro Miyazaki: Where do you situate “countering” in insurgent computing? How would you situate insurgent computing within countering and how do you imagine its role?

Anna Engelhardt: Countering is an intrinsic part of the genealogy of insurgent computing. The term “insurgency” was coined by military thinkers, who referred to their campaigns as those of “counterinsurgency,” legitimising with this term the violence they inflict. In this sense, insurgency never existed outside of the countering. The complex relations implied in this negation can be solved by either adding another negative prefix, i.e. “counter-counter-insurgency” (resistance to or negation of the imposed order), or by taking it out, i.e. “insurgency” (appropriation of existing fears of the stat projects). Insurgent computing connects those strategies, as reading RAND Corporation reports as aspirational cookbooks of what we are yet to achieve (*The Zapatista ‘Social Netwar’ in Mexico*) requires a critical lens attuned to constant filtering of practices that have to be abolished or will lead nowhere.

Shintaro Miyazaki: Could you please suggest further counter-Ns or N-computing(s) or N-futuring(s)?

Anna Engelhardt: decolonial computing, unorthodox computing (Rodrigo Ochigame), abolitionist computing (https://thenewinquiry.com/bail-bloc/)

Anna Engelhardt
Insurgent Computing

This publication is part of COUNTER-N, an online journal edited by Özgün Eylül İşcen and Shintaro Miyazaki. It is published electronically on the edoc-server of the Humboldt-Universität zu Berlin, https://edoc.hu-berlin.de/

Title: Insurgent Computing
Author: Anna Engelhardt
Editors: Özgün Eylül İşcen, Shintaro Miyazaki
Graphic Design: Ahmet M. Öğüt
Published in 2022 by counter-n.net

DOI: doi.org/10.18452/24455
Final Submission: October 21, 2021