

Automated Genocide

Written by Jingwen Wu and Matthew Penn

This PDF is auto-generated for reference only. As such, it may contain some conversion errors and/or missing information. For all formal use please refer to the official version on the website, as linked below.

Automated Genocide

<https://www.e-ir.info/2024/07/04/automated-genocide/>

JINGWEN WU AND MATTHEW PENN, JUL 4 2024

The world is in the middle of a new major technological revolution. To be specific, this is the third major technological revolution in the last 35 years. Starting with the creation of the World Wide Web in 1989, information was put online, and it could be accessed across the world at the speed of electrical signals. This was the information revolution. Despite this major innovation, information was largely unstructured and difficult to access. In the late 90s and early 2000s, online information became more structured. Advanced search engines, like Google, came online. Social media sites, like Myspace and Facebook, went online. This was the data revolution. Information became more accessible, structured, and abundant, but the large amounts of raw data was difficult to manage, sort, and turn into actionable intelligence. Starting in the late 2000s to the present day, innovations like online crowdsourcing, advances in artificial intelligence, facial recognition, social media data mining, and gamification have enabled massive amounts of data to be processed into intelligence quickly and efficiently. This is the intelligence revolution.

These same advances in technology that have enabled the intelligence revolution have also enabled governments to deploy enormous capabilities that were never possible before. If mass surveillance technology, advanced targeting systems, autonomous drones, and advanced artificial intelligence were combined together, governments could create a lethal capability beyond even Orwell's gravest prophecies. In other words, governments could create systems of automated genocide. How would such a system work?

The first stage of a system of automated genocide is mass surveillance, both in the physical and cyber battlespaces. Mass surveillance technology enables the linking of massive amounts of cameras across very wide geographic areas to monitor entire populations. Using facial recognition, states can easily identify and track people using these mass surveillance systems. China is currently using this technology to horrible effect in Xinjiang to identify and monitor the Uighurs. Israel uses a mass surveillance system called Red Wolf to track Palestinians using facial recognition.

Cyber data mining has also grown far more sophisticated and powerful. Ever since the invention of the internet, governments have been using advanced data mining programs to monitor their respective populations. For example, the Federal Bureau of Investigation's Carnivore program was an early example of government data mining, and Carnivore's capabilities were surpassed by the National Security Agency's PRISM program, which captured massive amounts of data from across the internet. The creation of social media has only made this process easier. Bots and other advanced scrapers guided by artificial intelligence can easily data mine countless social media profiles, posts, and other pieces of media to gather intelligence on dissidents and political activists.

Cambridge Analytica demonstrated the capabilities of data mining software during the 2016 Presidential Election when they data mined 87 million Facebook profiles. LinkedIn, Facebook, and Twitter profiles alone contain treasure troves of information: names, addresses, locations visited, phone numbers, emails, profile pictures (for facial recognition), education, places of employment, and the names of coworkers and friends. Social media profiles also contain information that could serve as various metrics for a government looking for dissent: connections to other dissidents (Facebook friends, LinkedIn connections, Twitter followers, etc.), Tweets, Twitter hashtags, and Facebook comments. A mass surveillance system could use social media data to build a massive social network map and profiles of political dissidents.

Mass surveillance is not just about cameras, cyber data mining, and electronic listening devices, though. Human

Automated Genocide

Written by Jingwen Wu and Matthew Penn

intelligence (HUMINT) still plays a vital role in any mass surveillance system, and technology can make the collection of HUMINT far more effective and efficient through crowdsourcing. Crowdsourcing is the use of large groups of people to collect information through online platforms. Using crowdsourcing, governments can collect intelligence from thousands, hundreds of thousands, or even millions of informants quickly and efficiently. Crowdsourcing also allows government to direct large groups of supporters to respond to online dissent. The Israeli government developed an online program called Act.il that facilitates the coordination of, "...thousands of mostly U.S.-based volunteers who can be directed from Israel into a social media swarm." This app allows the Israeli government and its allies to promote their narratives and respond effectively to any counter-narratives.

Using this data, governments could identify dissidents, opposition political activists, and any other groups that could pose a threat to the regime. Using a gamification system (similar to the social credit system used in China), these people can be ranked according to many different metrics (e.g., ties to other dissidents, work with dissident groups, participation in protests, etc.) to determine their threat level. With this ranking, governments can focus their mass surveillance system to target specific individuals for continuous monitoring. As more intelligence comes into the system, each target's individual ranking can change based on the target's evolving threat profile.

Once a targeted individual has reached a certain ranking, the system will automatically begin creating a plan to neutralize the threat. At lower thresholds, the system might only dispatch bots to troll a target's social media accounts. At a higher threshold, the system might dispatch security forces to incarcerate or deport the target. At the highest threshold, the system could dispatch autonomous drones, using the most advanced "swarm drone" technology, to assassinate the target.

This type of system is called an automated kill chain, and it is not science fiction. The United States military has been developing this technology for years to target Al Qaeda and ISIS militants. Israel has already fielded an automated kill chain called Lavender in Gaza. Lavender combines data mining with a gamification algorithm to rank and designate targets for bombings and assassinations. Where's Daddy is another system deployed by Israel in Gaza, and it uses integrated mass surveillance to track targets. The Ukrainian government is using an automated kill chain program called MetaConstellation. MetaConstellation combines, "...commercial and classified government data...which allows military officials to communicate enemy position to commanders on the ground or decide to strike a target."

Right now, the steps of the kill chain still have some degree of separation and human involvement at each stage. For example, Israel's Lavender target ranking system is separate from the Where's Daddy militant tracking system, and these systems still require human commanders to order strikes from drones or other military assets. To completely automate a kill chain, an advanced artificial intelligence that can effectively process the massive amounts of data is needed, and it is only a matter of time before someone develops the artificial intelligence necessary to run such a system.

When such a powerful and dangerous weapon becomes feasible, its creation becomes virtually inevitable. When nations do begin fielding completely automated kill chain systems, these systems will simultaneously monitor, target, and eliminate dissidents across entire populations. Yes, humans will still be involved with the collection and analysis of intelligence at various points along the kill chain, but the process, from data mining to target acquisition to execution, will be automated.

These systems for automated genocide will be the 21st century's new weapons of mass destruction. Unlike the indiscriminate destruction of nuclear weapons, systems for automated genocide can target tens of thousands, hundreds of thousands, or even millions of selected people belonging to specific groups (political dissidents, opposition groups, ethnic minorities, etc.) with a high degree of precision and lethality, which creates an unparalleled threat in today's world. In the six months since Israel's war in Gaza started, the Israeli military has killed 33,137 Palestinians, and many of these deaths were the result of Israel's Lavender and Where's Daddy targeting systems. Imagine how high the death toll would have been if the Israeli military had a completely automated kill chain.

Automated genocide is not just a concept from science fiction or Orwell's nightmares. Automated genocide is a

Automated Genocide

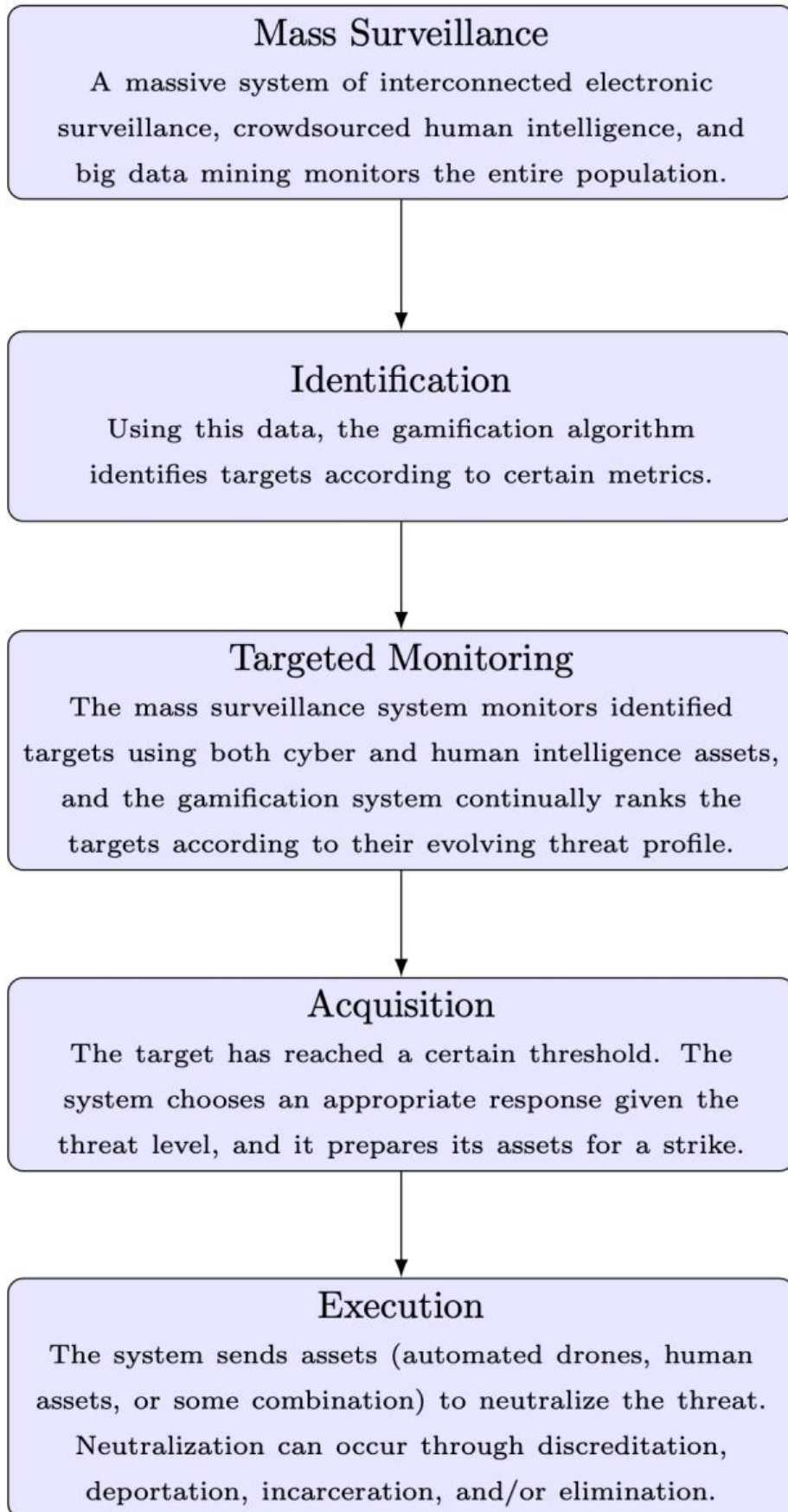
Written by Jingwen Wu and Matthew Penn

product of the intelligence revolution, and it is the result of the failure of both international and domestic legal frameworks to regulate and curb the misuse of these emerging technologies. The technologies that will enable automated genocide are not theoretical; these technologies have been developed and are currently being applied. The only missing piece is the integration of these technologies with artificial intelligence to enable a fully automated kill chain. The integration of artificial intelligence, crowdsourcing, gamification software, facial recognition, and swarm drone technology will allow governments to kill at a speed and efficiency never before seen in world history. Without the establishment of a global regulatory body to oversee the development and spread of these destructive tools – like the worldwide stance on nuclear weapons – the world is looking at the proliferation of a terrifying new weapon of mass destruction.

Figure 1

Automated Genocide

Written by Jingwen Wu and Matthew Penn



Automated Genocide

Written by Jingwen Wu and Matthew Penn

About the author:

Jingwen Wu is a PhD candidate at the University of Kentucky. She has published academic papers on the impact of 5G technology and human rights.

Matthew Penn is an open-source intelligence analyst with a master's degree in European history. Formerly, he was a recruiter and project manager at the crowdsourced consulting firm Wikistrat.