ARMY CYBER INSTITUTE AT WEST POINT PRESENTS

HIDDEN STRATAGEM

MICROTARGETING: THE FUTURE OF CONFLICT


THE ARMY CYBER INSTITUTE AT WEST POINT
·2012·

INTRODUCTION:

MICROTARGETING AS INFORMATION WARFARE

MAJOR JESSICA I. DAWSON, PH.D.
ASSISTANT PROFESSOR
ARMY CYBER INSTITUTE

In September 2020, General Paul Nakasone, NSA Director and Commander of U.S. Cyber Command, called foreign influence operations "the next great disruptor."[1] Nearly every intelligence agency in the United States government has been sounding the alarm over targeted influence operations enabled by social media companies since at least 2016, even though some of these operations started earlier. What often goes unstated and even less understood is the digital surveillance economy underlying these platforms and how this economic structure of trading free access for data collection about individuals' lives poses a national security threat. Harvard sociologist Shoshana Zuboff calls this phenomenon "surveillance capitalism [which] unilaterally claims human experience as free raw material for translation into behavioral data."[2] This behavioral data is transformed into increasingly accurate microtargeted advertising.[3] The new surveillance capitalism has enabled massive information warfare campaigns that can be aimed directly at target populations. The predictive power of surveillance capitalism is not only being leveraged for advertising success but increasingly harnessed for mass population control[4] enabled by massive amounts of individually identifiable, commercially available data with virtually no oversight or regulation.

This is not to say there is no oversight—data use and collection by the intelligence community is subject to significant oversight and regulation. This is not about data use laws and areas that are already regulated. Technology companies such as Facebook or Google exist in ungoverned spaces and are not subject to regulations like specific industries such as banking, education, or health care providers. For example, medical companies are clearly bound by the Health Insurance Portability and Accountability Act (HIPAA) and the banking industry is bound by Sarbanes Oxley, which includes data regulation components. Conversely, the tech companies actually have a shield from liability based on the Communications Decency Act, Section 230.[5] This law places tech companies outside of regulatory restrictions rather than

providing any meaningful limit on their actions and, as a result, creates a national security risk for the Department of Defense (DOD).

> **FUNDAMENTALLY, DOMESTIC DIGITAL PRIVACY IS A NATIONAL SECURITY ISSUE. THE DOD SHOULD PLACE GREATER EMPHASIS ON DEFENDING SERVICE MEMBERS' DIGITAL PRIVACY AS A NATIONAL SECURITY THREAT.**

For example, Facebook has acknowledged its platforms'* abilities to help political campaigns target voters to defeat ballot initiatives[6] and, more recently, Channel 4 News in the United Kingdom reported on how political action committees (PACs) in the U.S. targeted voters to decrease opposition turnout using the Cambridge Analytica dataset. [7] These incidents and others have caused people to look at the concentrated power companies leveraged via these platforms. One can argue microtargeting allows individual-level messaging to be deployed to influence voting behavior and is able to be leveraged for more insidious dis/misinformation campaigns. What started as a way for businesses to connect directly with potential customers has transformed into a disinformation machine at a scale that autocratic governments of the past could only imagine. The U.S. must recognize the current advertising economy as enabling and profiting from information warfare being waged on its citizens and address the threat.

Fundamentally, domestic digital privacy is a national security issue. The DOD should place greater emphasis on defending service members' digital privacy as a national security threat. This is not a hypothetical issue. China recently accused a staff sergeant of being patient zero in the COVID-19 pandemic, which unleashed a torrent of attacks online against her.[8] The targeting of key individuals by foreign agents has always been a national security threat, yet the current advertising ecosystem is not currently widely recognized as an attack space. Consider a defense contractor that targets a senior military leader in order to sway his/her decision on an acquisition. What if a missile systems operator is identified and targeted for digital blackmail by North Koreans? Worse, consider if China is successful in convincing key U.S. military officers that it poses no threat in the Pacific, leading to changes in the force posture that work to China's benefit. The murder of a Mexican American soldier and subsequent social media outrage at Fort Hood in 2020 demonstrates the impact a local incident can have on the national scale. All of this is enabled, with surgical precision, by the microtargeting advertising environment, fed by data gathered through apps, cell phones, games, and more.

This graphic novel is meant to illustrate the risks from microtargeting and the small, almost imperceptible actions that can shift the outcome of major events. Particularly in competition, the risks from commercial data collection and the weaponization of it towards adversary ends can shift momentum over a series of small movements. Supply chain disruptions can appear to be an accident, almost normal friction. Family members can be targeted to influence a key decision-maker. A long-term employee leaving for a better-paying job doesn't render any alarms. A frustrated idealist can trigger a national security event because of what they're consuming online – all individually targeted through algorithms enabled by commercial data collection.

The threat from microtargeting isn't a massive open wound. Instead, it's death by a thousand cuts from an unseen knife.

SCIENCE FICTION PROTOTYPES are science fiction stories based on future trends, technologies, economics, and cultural change. The story you are about to read is based on threatcasting research from the Army Cyber Institute at West Point and Arizona State University's Threatcasting Lab. The story does not shy away from a dystopian vision of tomorrow. Exploring these threats inspires us to build a better, stronger, and more secure future for our Armed Forces.

ARMY CYBER INSTITUTE AT WEST POINT PRESENTS

HIDDEN STRATAGEM

MICROTARGETING: THE FUTURE OF CONFLICT


7 DAYS AGO. THE ATROPIAN SEA.
ANXIOUS TO TAP INTO THE SEA FLOOR'S RARE EARTH DEPOSITS, ATROPIA AGREED TO A JOINT VENTURE WITH ARN INDUSTRIES, A GLOBAL TECH GIANT.
THE ATROPIAN DEEP-SEA EXPEDITIONARY FORCE DESPERATELY NEEDED WORLDWIDE SUPPORT FOR THE COUNTRY'S RENEWABLE ENERGY PROJECTS
THE SUBMARINE KASTEL ROGER WAS ON ITS MAIDEN VOYAGE, TESTING AN EXPERIMENTAL NUCLEAR BATTERY, WHEN SOMETHING WENT WRONG...
WHAT HAPPENED TO THE POWER? INDICATORS SHOW THE BATTERY IS DEAD, BUT THE BATTERY CAN'T BE DEAD!
BATTERY
IT'S WORKING MA'AM ...
...THE SUB IS OUT OF THEIR CONTROL.
I CAN'T DO ANYTHING WITH HER!


WHAT DO WE DO NOW?
NOTHING IS WORKING!
CRACK!
WHAT WAS THAT?!
WE'RE GOING DOWN! WE'RE DEAD IN THE WATER!


TRACING SUBARINE:
KASTEL ROGER (LOST)
DANGER!
KASTEL ROGER THIS IS WILDCAT 3. CAN YOU HEAR US? REPORT. KASTEL, I REPEAT ...
COMMS ARE DOWN! SOMEONE PLEASE HELP US!
MA'AM, THE SUB HAS LOST ALL POWER AND IS COMING TO REST ON THE OCEAN FLOOR.
ALL ACCORDING TO PLAN. ALERT COMMAND OF OUR SUCCESS ...


... AND LET'S MOVE TO PHASE 2.


HIDDEN
STRAT


AGEM

THE WORLD OF 2030

suffered from splintered technological systems and isolated financial systems. There were those that aligned with a rules-based international order that served as a "check on power" and those that sided with an international order that rewarded the powerful. The Internet was fractured between these two systems: one system that devoured every bit and byte of available data for surveillance of people and systems and one that used claims of better data in order to improve people's lives. These rivalries were joined on the world stage by a new generation of super-empowered individuals, organizations, and other non-traditional actors, ranging from technology billionaires who claimed to want to save the world to terrorist networks who wanted to create chaos. Groups–sometimes unknowingly–manipulated people at scale through the use of targeted digital media. Far more than just a modern gloss on classic advertising, the influence machinery is wide-reaching and inescapable. A continuous collection of data enables more precise targeting than previous generations could have ever imagined.

Exhausted by the widespread death and destruction throughout the 2020s, a short-lived, tenuous peace was created by way of a targeted digital marketing campaign encouraging people away from violence and toward peace and harmony. These efforts focused less on clear, legible military targets and more on civil and private infrastructure and institutions, such as healthcare, agriculture, and energy – leading to peace but also a loss of freedom and agency because the systems were always watching. Global surveillance giants slowly degraded the state military capacity by convincing the young not to join the military and that peace could be attained without violence. They convinced the older generations that prosperity could be gained through stability, not war. The use of data collection from all facets of daily life resulted in the expansion of disruptive technologies. This allowed for broader multifaceted surveillance across domains and controls of targets to an extent not yet seen.

Cyberspace became more fragmented as authoritarian states imposed sovereign digital controls and aimed to separate from the global Internet. They did this in the name of protecting their people from foreign influence, but that was only half the story. The other half was that by controlling the information, these authoritarian regimes demonstrated how much they did not trust their people. In fact, they worsened the existing social fragmentation and further eroded basic prosperity and security. This led to increased unrest among those who were not hyper-connected. This fed an overarching trend of volatility and instability around social norms. Institutions whose resilience was once taken for granted were no longer trusted. The primary threat to both democratic society and rules-based international order was the return of "strong man rule." Those "strong men" used data in new ways to remove any obstacles to their objectives through both legal and extralegal means. Those compelled by this form of "strongman" governance repeatedly tested the adaptability of our interconnected global systems–disrupting institutions that refused to comply with their demands. Targeted information manipulation created confusion around who was doing what, enabling these techno-dictatorships to rule in their sphere of influence unchallenged.

The economic transition from buying things to subscribing to things was also nearly complete. Most of the global economy no longer enabled people to buy things outright–subscriptions were often the only option, and while that appeared cheaper for the end user, it came with a cost: continued data extraction from "always on" technology. Software as a service and subscription to daily life relentlessly collected data on the world, becoming more deeply embedded in physical systems. By transitioning to computerized systems as opposed to more "offline" mechanical systems, new vulnerabilities expanded cyberwarfare attack surfaces to an unprecedented degree. Those systems that maintained mechanical capabilities remained more resilient to cyberattacks/espionage, but the global data giants continually worked to undermine these capabilities–if they couldn't collect data, they couldn't control it. The interconnected world of 2030 was buggy, brittle, and easily hacked. But the prevailing view was that if you had nothing to hide, there was no need to worry about the constant invasion of privacy, whether it came from tech companies or government institutions. But this view was fundamentally wrong.

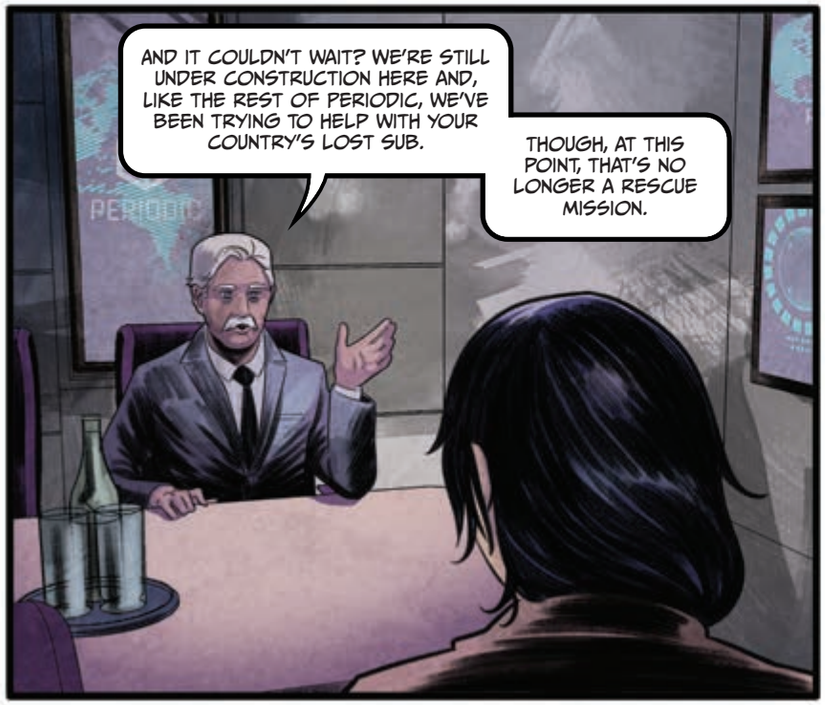
Artificial Intelligence (AI) made tremendous gains in the intervening decades and was used to compile everything, to "zero in" on the weakest individual in an organization who could become a single point of failure. The rapid advances in biocomputing empowered people to an unprecedented degree, granting them access to digitally augmented decision-making capabilities that were unthinkable only a few short years ago. As with every technology, there were those who benefited from it and those who were exploited by it. In the early 2000s, Periodic, a Silicon Valley technology platform, rose to global dominance by figuring out how to encode the analog world into digital code. They used videos, memes, social media, and games to extract data about the emotions of their users. Their platform could determine what made someone more likely to trust someone else. Periodic identified what information or "nudges" would motivate its users to take a small, out-of-the-ordinary action that was not only betraying their own groups, but also eroding broader social frameworks of trust and cohesion–things critical to the functioning of democracy. Periodic's global dominance went largely unchallenged. Yet, they missed something ...

By 2030, Periodic had gathered more data on more companies and individuals than any other company in the world. Their AI program, Gyges One, could analyze everything from supply-chain bottlenecks to an individual's personal vulnerabilities. In the run-up to 2030, Periodic started competing with ARN Industries to build a deep-sea mining prototype to help Atropia extract resources from the seabed. If successful, Periodic could reduce ARN Industries and Donovian dominance over rare-earth mineral extraction in the region. The world of 2030 was one in which technology, platforms, and their data threatened to exploit a connected world with a "strategic shock" that would leave it exceedingly fragmented.


TODAY, PERIODIC HEADQUARTERS, DONOVIA


I WISH YOU HAD CALLED AHEAD. I WOULD HAVE TOLD YOU THE TIMING COULDN'T BE **WORSE** FOR A MEETING.
AND, HONESTLY, I'M NOT TERRIBLY EXCITED ABOUT HAVING A **PRIVATE** MEETING WITH AN **ATROPIAN** AGENT.
YOU'LL UNDERSTAND WHY WE HAD TO MEET SOON ENOUGH. WE HAVE A LOT TO COVER REGARDING THE POTENTIAL OF OUR PARTNERSHIP ...
NO.18
REC.

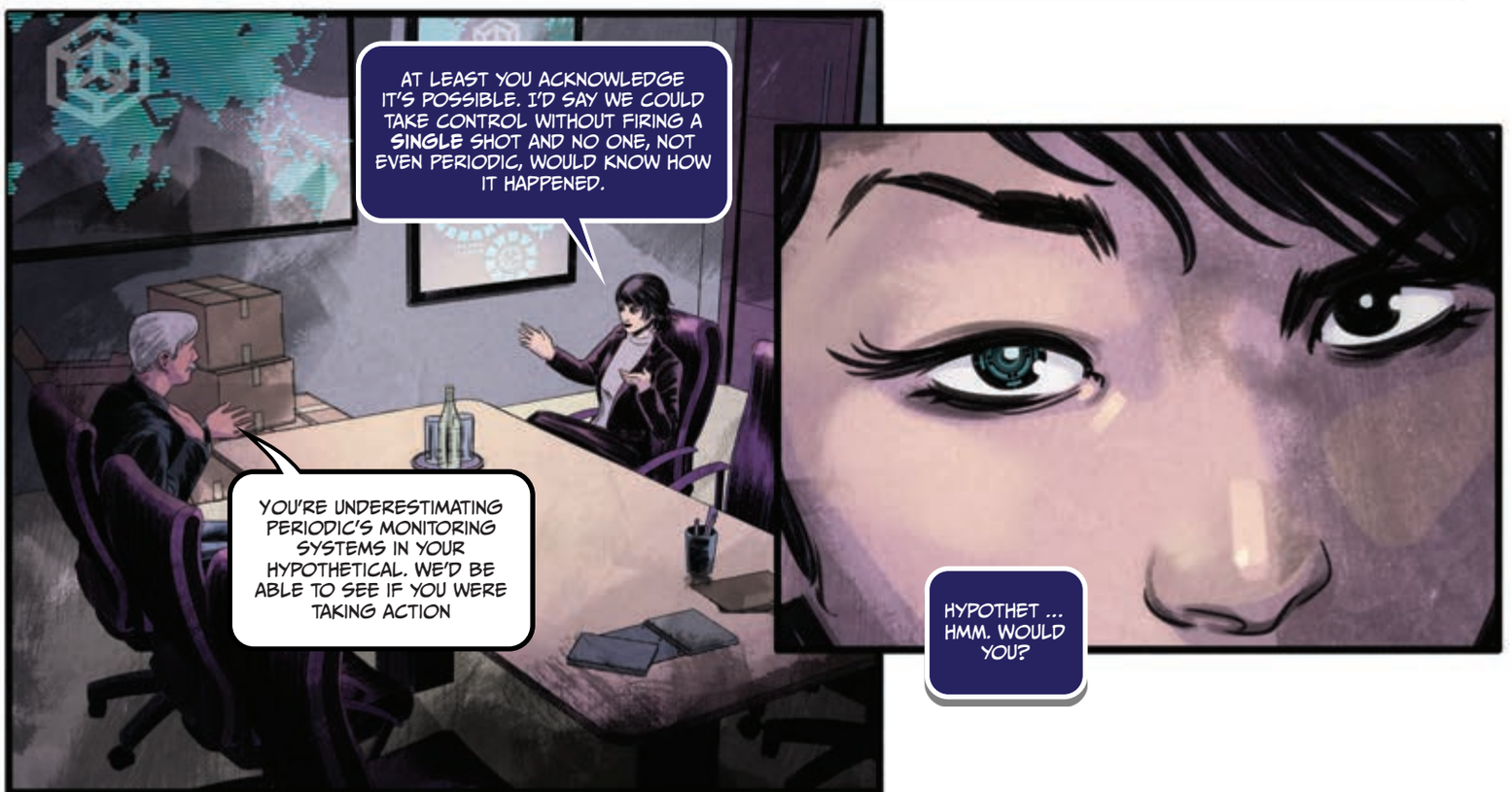

... AND THERE ARE SOME THINGS THAT ARE **BETTER** DISCUSSED IN PERSON.


AND IT COULDN'T WAIT? WE'RE STILL UNDER CONSTRUCTION HERE AND, LIKE THE REST OF PERIODIC, WE'VE BEEN TRYING TO HELP WITH YOUR COUNTRY'S LOST SUB.
THOUGH, AT THIS POINT, THAT'S NO LONGER A RESCUE MISSION.
PERIODIC

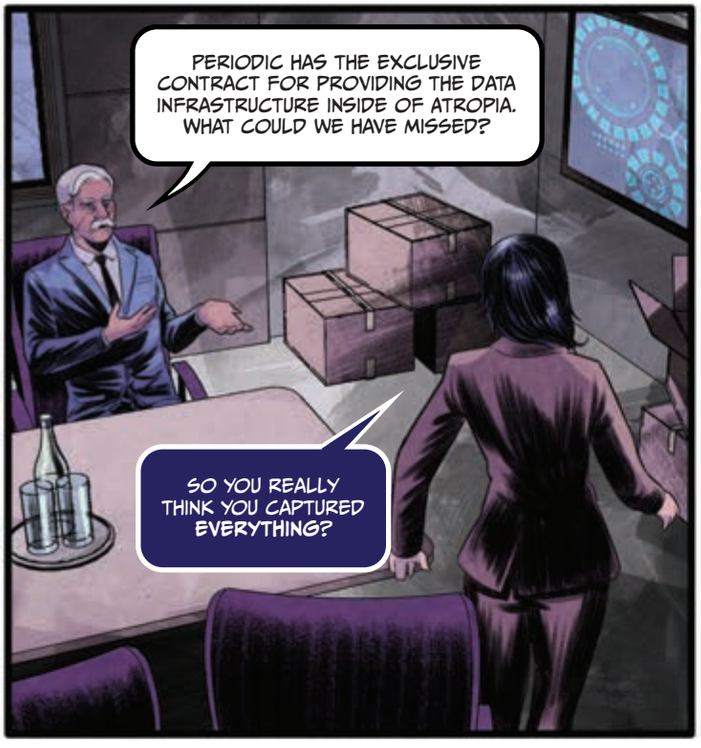

I CAN SEE WHY YOU'D THINK THAT.
LET'S SKIP THE PLEASANTRIES THEN. WE HAVE **MORE** TO DISCUSS THAN YOU REALIZE.

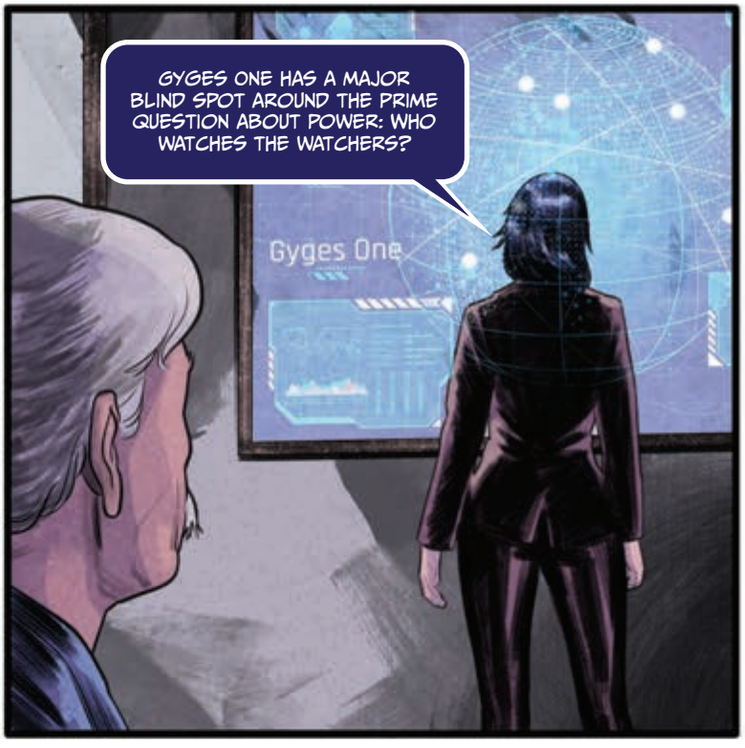

BEFORE YOU OFFICIALLY OPEN YOUR OFFICES HERE IN DONOVIA, THERE ARE THINGS YOU NEED TO KNOW ABOUT OUR RECENT SUCCESS.
AS YOU KNOW, THE ATROPIANS WERE DETERMINED TO DEVELOP THEIR OWN NATIONAL MINING OPERATIONS THAT WERE NOT DEPENDENT ON MULTINATIONAL CORPORATIONS. HOWEVER, **WE** HAD INTERESTS OF OUR OWN. SO WHEN THE ATROPIAN NATIONAL COMPANY **ARN** FOLDED, WE WERE THERE TO PICK UP THE PIECES.
THANKS IN NO SMALL PART TO PERIODIC'S SYSTEMS.
NO OFFENSE, BUT YOU'RE MISINFORMED. I'M VERY AWARE OF OUR SYSTEM'S CAPABILITIES, AND MINING INFRASTRUCTURE IS A BIT OUTSIDE OUR WHEELHOUSE.
NO OFFENSE TAKEN. WE'VE DEVELOPED A SUITE OF ARTIFICIAL-INTELLIGENCE TOOLS THAT DOVETAIL WITH PERIODIC'S IN WAYS YOU'VE NEVER CONSIDERED. BUT BEFORE WE GO INTO THAT ...
LET ME ASK YOU A QUESTION.
SAY YOU WANTED CONTROL OF ARN INDUSTRIES' MINING OPERATIONS, **AND** YOU WANTED ATROPIA'S RARE-EARTH MINERAL RIGHTS.


WHAT WOULD IT TAKE TO ERODE ARN INDUSTRIES' FRIENDLY RELATIONSHIP WITH ATROPIA? AND, AS A BONUS, THROW A WRENCH IN THE WEST'S PRESENCE AND RESEARCH OPERATIONS IN THE REGION. MAYBE EVEN SHINE A POSITIVE LIGHT ON DONOVIA?
DONOVIA
ATROPIAN SEA
ATROPIA
I'D SAY LOTS OF LUCK. YOU'D HAVE TO OVERCOME **GENERATIONS** OF DISTRUST BETWEEN ATROPIA AND DONOVIA. NOTHING'S IMPOSSIBLE, BUT THAT WOULD COME AWFULLY CLOSE.


AT LEAST YOU ACKNOWLEDGE IT'S POSSIBLE. I'D SAY WE COULD TAKE CONTROL WITHOUT FIRING A **SINGLE** SHOT AND NO ONE, NOT EVEN PERIODIC, WOULD KNOW HOW IT HAPPENED.
YOU'RE UNDERESTIMATING PERIODIC'S MONITORING SYSTEMS IN YOUR HYPOTHETICAL. WE'D BE ABLE TO SEE IF YOU WERE TAKING ACTION
HYPOTHET ... HMM. WOULD YOU?


IF YOUR QUANTUM GYGES ONE SYSTEM IS CONNECTED TO **EVERYTHING**, YOU CAN'T POSSIBLY DEFEND IT ALL... BELIEVE ME, THERE ARE CERTAINLY SOME THINGS THAT YOU MISSED.
A FEW MORE SECONDS AND IT WILL BE CONNECTED ...


PERIODIC HAS THE EXCLUSIVE CONTRACT FOR PROVIDING THE DATA INFRASTRUCTURE INSIDE OF ATROPIA. WHAT COULD WE HAVE MISSED?
SO YOU REALLY THINK YOU CAPTURED **EVERYTHING**?


GYGES ONE HAS A MAJOR BLIND SPOT AROUND THE PRIME QUESTION ABOUT POWER: WHO WATCHES THE WATCHERS?
Gyges One


WE SPENT MONTHS MONITORING ARN ... BUT IT WAS YOUR SYSTEM THAT GAVE US UNPARALLELED ACCESS TO SO MANY PIECES OF THE PUZZLE.
YOU ENGAGE PEOPLE'S EMOTIONS – YOUR SYSTEM, MORE THAN ANYTHING OUT THERE, KNOWS WHAT MAKES PEOPLE TICK. WE JUST HAD TO COMBINE IT WITH OTHER INFORMATION TO GET THE RESULTS WE DESIRED.
WITH DISTRACTIONS AVAILABLE 24-7 ON YOUR PHONE, FUN ISN'T MERELY FUN ... WITH THE RIGHT EYES ON CAT VIDEOS AND FANTASY FOOTBALL, "FUN" BECOMES OUR GATEWAY TO INDUSTRIAL ESPIONAGE.

OPEN-SOURCE DATA IS EVERYWHERE—EXCEPT THE ARMY'S CONCEPT OF INFORMATION ADVANTAGE

MAJ Maggie Smith and MAJ Nick Starck

Originally published as part of the Army Cyber Institute's/Modern War Institute's Competition in Cyber Project [https://mwi.usma.edu]
05.24.2022

Three months ago, as Russia invaded Ukraine, the world watched as Twitter exploded with real-time data, reporting, and analysis of the unfolding conflict. It quickly became clear that the war presented analysts with an unprecedented amount of rich, open-source data on military movements, troop location, shelling damage, weapon types, and more. Ukraine has been quick to capitalize on Russia's poor data protection, and President Volodymyr Zelenskyy has become Ukraine's most potent weapon because of his ability to use data and information and Russia's inability to protect it.

For the U.S. Army, a key takeaway from the Ukrainian conflict so far should be the extent to which our modern-day habits are trackable, traceable, and predictable. Open-source data presents modern militaries, especially wealthy high-tech ones, with a very uncomfortable truth: militaries are exposed because their troops are connected. Currently, the U.S. legal and regulatory systems do not, and cannot, protect the average citizen—and therefore, the average U.S. service member—from risks associated with the ubiquitous open-source data produced by our surveillance economy. From a national security perspective, the accumulation of open-source data on people—their habits, their likes and dislikes, their exercise routines, and more—and its potential to impact the military's ability to fulfill its man, train, and equip mandate from Congress is deeply concerning. Also alarming is the amount of information our adversaries can glean about U.S. strategic interests from tracking U.S. military activity on any number of apps, like Flightradar24, which includes U.S. military reconnaissance platforms such as the unmanned RQ-4 Global Hawk, the RC-135V Rivet Joint, and others among the aircraft it tracks, and Strava, the fitness tracking app. Ultimately, you can intuit quite a bit about where our forces may be heading, where military planners are focusing their efforts, and where the next conflict is likely to occur if you simply track where Rivet Joints are conducting sorties and service members are working out. And for the Army specifically, the existing and emerging doctrine fails to account for the surveillance economy and its open-source data, leaving a gaping hole in our competitive strategy.

Information Advantage: What Is It?

Presently, the Army is developing its doctrine for its newest term of operational art: information advantage. Information drives friendly, neutral, and adversary actors at all levels and across all domains of warfare. Information advantage is a condition of relative advantage that enables a more complete operational picture and leads to decision dominance—the sensing, understanding, deciding, and acting faster and more effectively than the adversary. Gaining the initiative and maintaining a position of relative advantage over the information environment—regardless of where we find ourselves on the conflict continuum—largely depends on a commander's ability to achieve an information advantage over a defined target audience or adversarial decision maker in a specific context or timeframe. Complementary to information advantage is the employment of

information and other capabilities as weapons designed to shape friendly, neutral, and adversarial perceptions, attitudes, and behaviors. Ultimately, the ability to shape perception and achieve victory in modern conflict and competition is heavily dependent on trust—trust in data, among team and unit members, in leaders, in doctrine, in equipment, and in capabilities.

To achieve information advantage, the Army conceives of five interrelated core tasks—what have been described as "information advantage activities." Commanders must: 1) enable decision making; 2) protect friendly information; 3) inform and educate domestic audiences (a task conducted in accordance with laws and focused on public affairs office activities); 4) inform and influence international audiences; and 5) conduct information warfare. In theory, information advantage activities are synchronized through the operations process, integrated across the Army's six warfighting functions—command and control, intelligence, protection, movement and maneuver, fires, and sustainment—and employed using all available military capabilities. After distilling the Army's rhetoric, information advantage requires commanders to prioritize persistent sensing, ongoing analysis, cyclical assessments, and a willingness to continuously update assumptions to ensure they maintain a dynamic situational awareness of the environment—in competition and conflict. Ultimately, the Army anticipates that victory in future warfare, and in the current era of persistent engagement, will come down to who can gain the most by effectively employing information to their advantage.

"The ability to shape perception and achieve victory in modern conflict and competition is heavily dependent on trust—trust in data, among team and unit members, in leaders, in doctrine, in equipment, and in capabilities."

The National Security Risk

Instead of gunfire or artillery explosions, some of the first signs that Russia was invading Ukraine on February 24, 2022, came from Twitter. For example, Dr. Jeffrey Lewis, an expert in arms control and nonproliferation, compiled open-source data from the traffic layer of Google Maps and shared the Russian troop movements he identified, essentially in real-time, on Twitter. According to Google Maps, he tweeted, "there is a 'traffic jam' at 3:15 in the morning on the road from Belgorod, Russia to the Ukrainian border"—exactly the spot where vehicles, equipment, and manpower had massed the previous day. "Someone's on the move," Dr. Lewis concluded, and he was right. As the Ukrainian conflict escalated, individual researchers and organizations continued to collect and analyze open-source data—also defined as publicly available information by DOD—from social media platforms, commercial satellites, and public databases. Their analysis and reporting have emerged as a critical resource on the conflict, providing combatants and observers with incredible insight and minute-by-minute assessments of what is happening on the ground.

However, the ability to track ongoing military operations through open-source data is not new.In 2016, Bellingcat released a report that used open-source data to document the full scale of the Russian artillery attacks against Ukraine in the summer of 2014. In fact, using open-source data is the new normal. And various U.S. government agencies, including the Department of Defense, rely on open-source data for intelligence and procure data through contracts with data brokers. In response, civil society and privacy watchdogs around the world have voiced concern, highlighting the risks to personal privacy associated with government-led data collection, aggregation, and use. The likely result is new legislation, like the proposed Fourth Amendment is Not For Sale Act and others.

However, the use of open-source data and large-scale, legal data collection efforts frequently pose less obvious national security risks. China, for example, aggressively collects data—legally and illegally—to support its domestic and international goals. A major threat to U.S. citizen data is China's Beijing Genomics Institute (BGI), which has grown into one the world's largest genomic companies after working on the Human Genome Project. BGI developed a prenatal genetic test, in collaboration with the Chinese military, that is sold and used globally. However, in addition to providing prospective parents with important genetic information, the DNA specimens are also amassed into a vast bank of genomic data that China is using to conduct large-scale studies of population traits. More than eight million women have taken BGI's prenatal tests globally, and China has their DNA and location data stored locally in mainland China. BGI also developed a COVID-19 test and offered to set up testing laboratories in several U.S. states at the start of the pandemic. Mike Orlando, head of the National Counterintelligence and Security Center, identified the BGI offers as a national security risk, "citing concerns about how China might use personal data collected on Americans." Even when done legally, DNA collection by Chinese companies should be understood as part of China's comprehensive effort to collect records and data.

On the other hand, data also creates risk for the governments that aggressively pursue it. Experts are increasingly identifying the ways that open-source data can be used to expose government activity (e.g., military maneuvers, resource allocation, travel, or policy activity) and how the ever-growing pools of open-source data generated by modern societies pose a national security risk. But we lack precision in how we describe the sources, mechanisms, and outcomes of open-source data risks, preventing the development of a coherent mitigation strategy tailored to the national security context. Without a common understanding of risk, civilian and military leaders are unable to make informed and consistent decisions about open-source data, leading to strategic missteps and tactical knee-jerk reactions—like embedding code in the Free Application for Student Aid website that sends user information back to Facebook (the code has since been removed) or banning service members from using geolocation features on devices in deployed areas (e.g., fitness trackers).

What Is Information Advantage Missing?

The piece missing from the Army's information advantage framework is an awareness of how the persistent aggregation of open-source data in the surveillance economy impacts the Army's ability to achieve information advantage. Because the American public is subject to the surveillance economy, U.S. service members are, too. George Washington famously emphasized that "when we assumed the Soldier, we did not lay aside the Citizen" as a cautious reminder that soldiers are citizens first. Since service members live alongside and among the general population, service members and veterans are not only susceptible to the same targeted marketing the average

citizen experiences, but are actually the target of additional foreign manipulation and surveillance efforts. Soldiers, sailors, airmen, and Marines access social media platforms and online services just as civilians do. They also purchase items online, apply for credit cards online, do their taxes with online tax preparation tools, and surf the web just like their civilian counterparts. But unlike the civilian neighbors they barbeque with, they also fight the nation's wars. Open-source data is produced continuously by all service members as they go about their digitally connected lives alongside their civilian counterparts, making the surveillance economy an integral part of the information environment that commanders need to consider as they conduct information advantage activities.

> "Ultimately, the risks of open-source data are not an individual's problem, but an Army problem."

The military is beginning to understand the potential risks presented by open-source data, particularly in combat situations, partly because examples of how open-source data can expose military information abound—from troop location tracking on Tinder to tracking stolen AirPods to SIM cards revealing Russian troop locations in Ukraine. Of course, these known cases fit neatly within traditional operational security risks and are scenarios that senior military leaders can relate to—especially when open-source data is directly contributing to deaths on the battlefield or to the identification of war criminals. However, having a tactical appreciation of the open-source data risks during periods of declared conflict is not enough to achieve information advantage—the risks to military operations are present well before any decision to go to war is made and persist after conventional conflict ends. In fact, the risks are a constant factor in the current competition environment, making any ex post facto restrictions, regulations, or rules placed on deployment behavior inadequate and misguided. Changes need to happen at home, well before the deployment cycle begins. Failing to consider garrison operations and the ways that soldiers interact with the surveillance economy as part of the information environment that commanders need to consider for information advantage is a failure to understand when and where the vulnerabilities and threats to the force begin and a failure to account for our modern, digitally connected, human behavior.

The "So What" of Open-Source Data

For multi-domain operations, the Army frames the operating environment as including human, physical, and informational aspects. To be effective across the competition continuum, the Army proposes positioning formations and capabilities forward so that information advantage activities are integrated into security cooperation efforts and crisis action planning on behalf of theater commanders. To coordinate information advantage activities in an area of conflict, the Army identifies that preparation must begin in competition, or when forces develop the intelligence to identify specific vulnerabilities and then gain or prepare to request the required authorities, and train to use national-level capabilities. The overall goal is operational convergence with formations postured to degrade, disrupt, or destroy adversary capabilities while defending those of friendly forces. However, what this framework does not consider is the intersection of the human, physical, and informational aspects or the risks to day-to-day garrison operations from open-source data.

Ultimately, the risks of open-source data are not an individual's problem, but an Army problem. For example, fake accounts on Facebook for U.S. Army general officers are numerous, and in some cases, fail to violate Facebook's terms of service and can therefore remain active. Even LinkedIn is rife with fake profiles attempting to make connections with users in targeted marketing campaigns. Additionally, fake social media accounts managed by Russia have already mobilized the American public in connection with divisive issues, making fake accounts for authoritative figures, like U.S. Army generals, especially concerning. From a national security perspective, open-source data enables foreign manipulation efforts that target the U.S. military and veteran populations through the use of "misleading and divisive questions about the U.S. government's military and veteran policies to further amplify and exploit the existing frustrations." The relative ease with which anyone can purchase open-source data means that soldier data is already being used to target service members for products, media, or other services, and presently, there is nothing preventing our adversaries from using open-source data to target them as well.

"As the Army develops its information advantage doctrine, it should simultaneously develop a dedicated data risk management framework to enable modern commanders to achieve information advantage."

To achieve information advantage, the Army needs to give commanders the tools necessary to assess the operational risks of open-source data, social media, and related information technologies. The Army has a longstanding doctrine for assessing operational risks; however, the traditional risk management framework is intentionally broad, leaving commanders without clear guidance or terminology for identifying, assessing, and making risk decisions in the information environment. As the Army develops its information advantage doctrine, it should simultaneously develop a dedicated data risk management framework to enable modern commanders to achieve information advantage. In its current form, information advantage perpetuates an antiquated notion that operating environments are (or can be) geographically bound. As the conflict in Ukraine has highlighted, kinetic actions may be limited to a geographic area, but informational risks are global. A dedicated data risk management framework would be a guide for commanders to continually and methodically assess the evolving information environment, to identify and address conceptual gaps, and to achieve their informational and operational goals. As the information environment emerges as the main effort in competition and conflict, the Army must adapt and provide its commanders with the right concepts, doctrine, and resources to succeed in a world characterized by the ubiquity of open-source data.

IDRIS DAVTYAN, REPRESENTATIVE [ATROPIA]

IMAGINE IF AN OPERATION COULD TARGET, SAY, ATROPIAN REPRESENTATIVE DAVTYAN AND TURN HIM AGAINST THE ARN PROJECT?

WITH ARN INDUSTRIES AS A PARTNER, THIS PROJECT WILL GIVE THE ATROPIAN PEOPLE MORE CONTROL OVER OUR MINERAL RIGHTS–AND THE ATROPIAN PEOPLE WILL BE THE PRIMARY BENEFICIARIES FOR GENERATIONS TO COME.

RIDICULOUS. DAVTYAN TESTIFIED TO THE ATROPIAN REGULATORY AGENCY ON ARN'S BEHALF. HE'S A TRUE BELIEVER.

YES, BUT HIS CHILDREN ... WHAT DO **THEY** BELIEVE IN?

WHEN THE NEWS ABOUT THE SUB BROKE, ATROPIANS WHO WERE ALREADY SKEPTICAL OF THE DEAL WITH A PRIVATE COMPANY TOOK TO THE STREETS. THEY REALLY DIDN'T LIKE A NUCLEAR SUB BEING LOST IN THEIR WATERS.

BREAKING NEWS

PUBLIC PRIVATE FAILURE

NUCLEAR SUB LOST

OUR SEA

NO

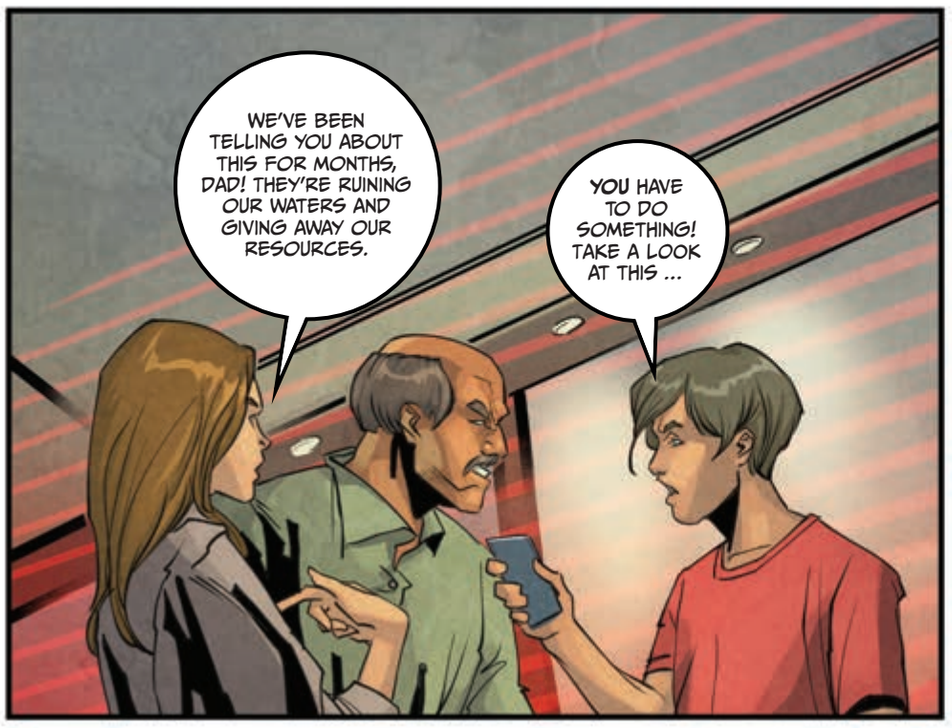
NUKES

DARMPY DAY

Family is Life's greatest blessing

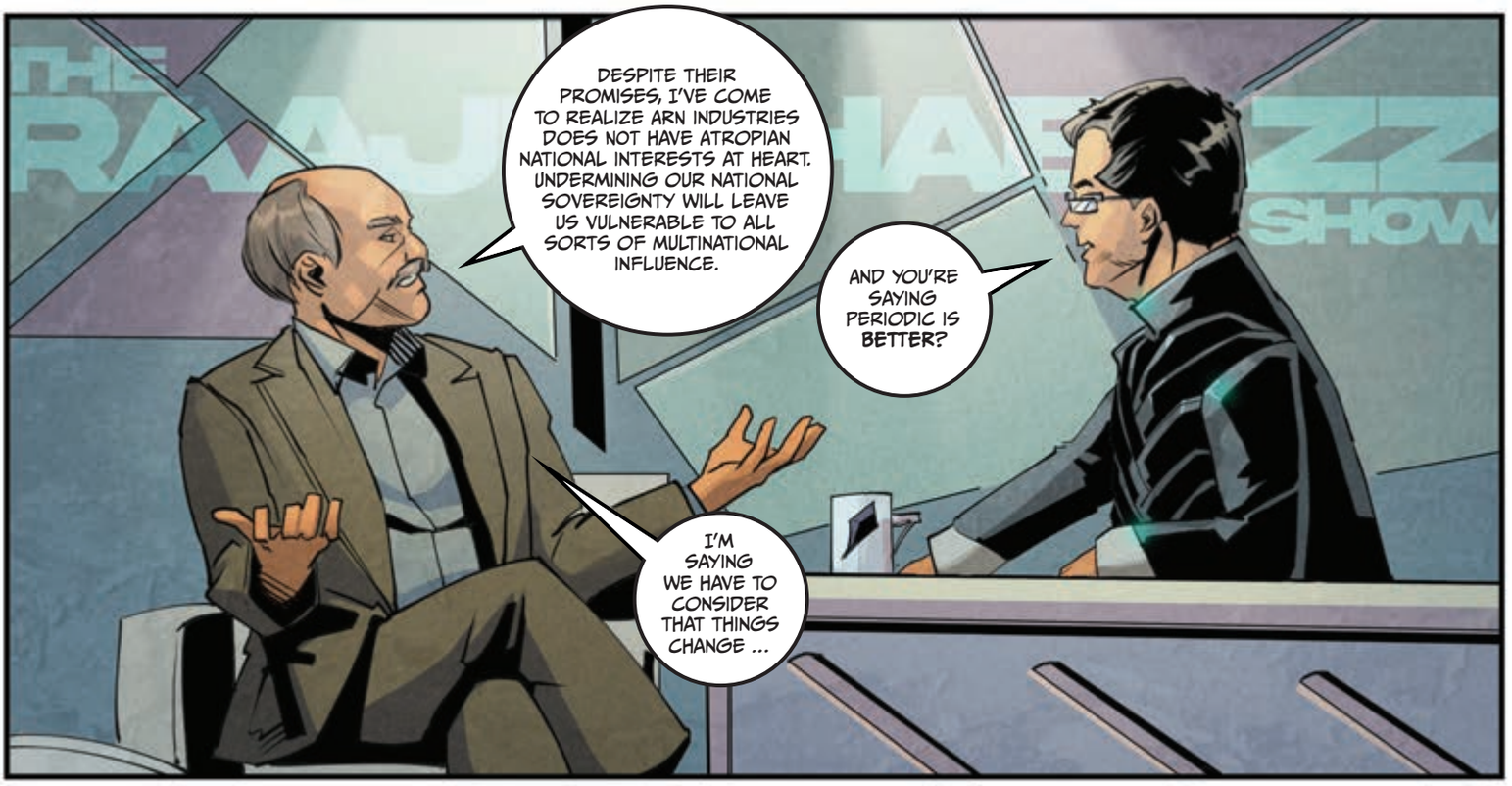
WITH SOMEONE AS COMMITTED AS DAVTYAN, A "FRIENDS AND FAMILY" APPROACH WOULD BE THE WAY TO GO. EVEN WHEN SOMEONE DOESN'T HAVE MUCH OF A SOCIAL MEDIA FOOTPRINT THEMSELVES ...

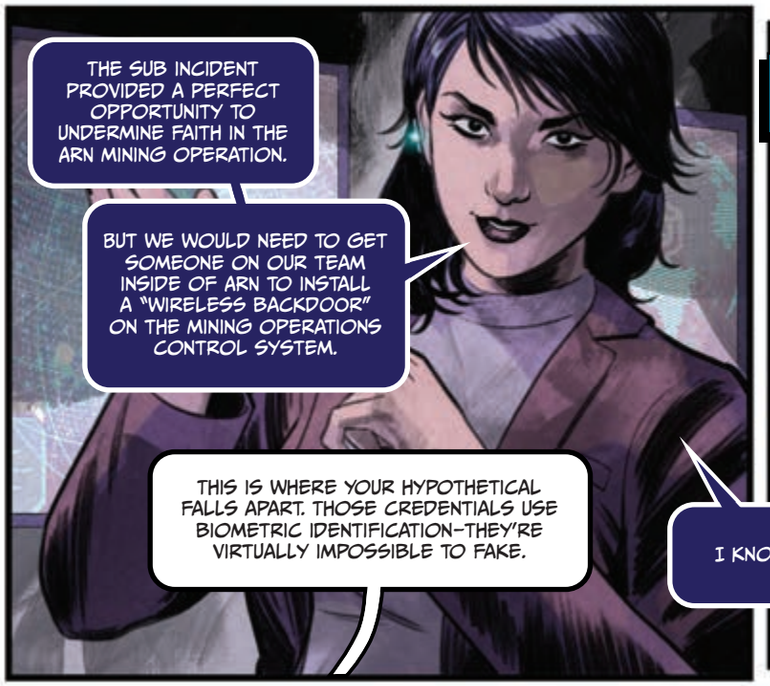

...YOU CAN USUALLY FIND SYMPATHETIC FAMILY MEMBERS. YOU'D BE SURPRISED AT HOW EXTREMELY EFFECTIVE THEY CAN BE AT RELAYING MESSAGING.
HIS CHILDREN, ALREADY POSITIVELY INCLINED TOWARDS THE ENVIRONMENT, COULD EASILY BE INDOCTRINATED INTO AN ANTI-ARN, PRO-ATROPIAN MOVEMENT, BECAUSE THEY BELIEVED IT WAS THE ONLY WAY TO SAVE THEIR FUTURE.
PROTECT OUR SEA!
WITH AI SCANNING OF SOCIAL MEDIA POSTS AND POLICE SURVEILLANCE FEEDS, IT WOULD BE EASY TO FIND HIS CHILDREN AT A PROTEST. AND THEN, WITH A SIMPLE NUDGE HERE, A NEWS ALERT THERE ... THEY COULD BE TARGETED FOR ARREST.
OUT OF OUR WATERS
NO MORE
NO MORE
YOU CAN IMAGINE THEIR FATHER'S FRUSTRATION ... WITH HIS CHILDREN, YES, BUT EVEN MORE WITH THE GOVERNMENT HE HAD SERVED SO LOYALLY.
I KNOW MY CHILDREN HAVEN'T DONE ANYTHING WRONG. YOUR SUPERIORS ARE GOING TO HEAR FROM ME!


WE'VE BEEN TELLING YOU ABOUT THIS FOR MONTHS, DAD! THEY'RE RUINING OUR WATERS AND GIVING AWAY OUR RESOURCES.
YOU HAVE TO DO SOMETHING! TAKE A LOOK AT THIS ...


FOR SOME, WHEN PROPAGANDA COMES FROM AN ANONYMOUS SOURCE, IT CAN EASILY BE IGNORED. BUT A CONCERNED, DEVOTED FATHER, SHOWN EVIDENCE BY HIS IMPASSIONED CHILDREN ...
THIS CAN'T BE RIGHT. WHERE DID YOU GET THIS?
...THAT'S ANOTHER MATTER ENTIRELY.

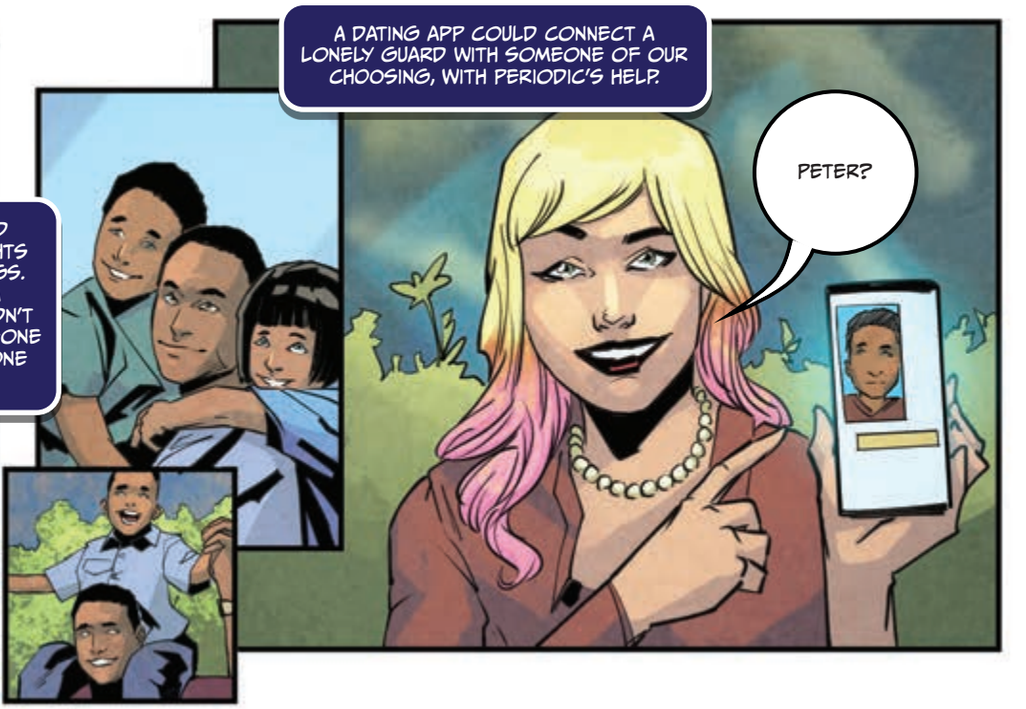

HE WAS SHOWN "NEWS STORIES" BY HIS OWN CHILDREN THAT "PROVED" FOREIGN INVESTMENTS HAD UNDERMINED DOMESTIC INDUSTRIES AND THAT ARN INDUSTRIES WOULD TAKE ITS PROFITS AND RUN, DECIMATING THE MANUFACTURING BASE WHEN IT LEFT.
I'LL HAVE TO LOOK INTO THIS. IF THIS IS TRUE ...


DESPITE THEIR PROMISES, I'VE COME TO REALIZE ARN INDUSTRIES DOES NOT HAVE ATROPIAN NATIONAL INTERESTS AT HEART. UNDERMINING OUR NATIONAL SOVEREIGNTY WILL LEAVE US VULNERABLE TO ALL SORTS OF MULTINATIONAL INFLUENCE.
AND YOU'RE SAYING PERIODIC IS BETTER?
I'M SAYING WE HAVE TO CONSIDER THAT THINGS CHANGE ...

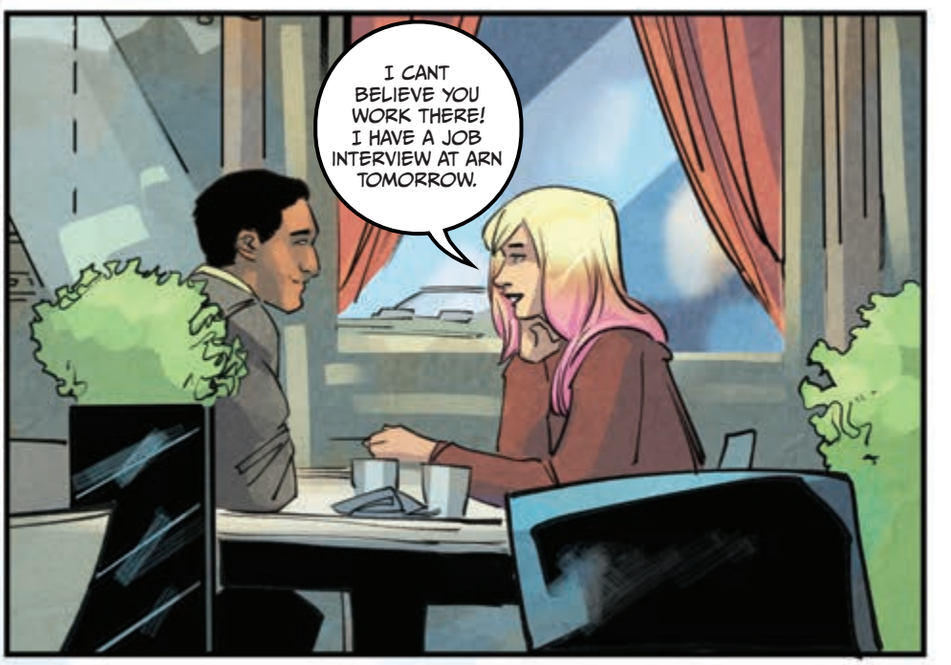

THE SUB INCIDENT PROVIDED A PERFECT OPPORTUNITY TO UNDERMINE FAITH IN THE ARN MINING OPERATION.
BUT WE WOULD NEED TO GET SOMEONE ON OUR TEAM INSIDE OF ARN TO INSTALL A "WIRELESS BACKDOOR" ON THE MINING OPERATIONS CONTROL SYSTEM.
THIS IS WHERE YOUR HYPOTHETICAL FALLS APART. THOSE CREDENTIALS USE BIOMETRIC IDENTIFICATION–THEY'RE VIRTUALLY IMPOSSIBLE TO FAKE.
I KNOW.


PETER GONZALEZ, SECURITY GUARD
[FRONT GATE TO ARN MINING HQ, ATROPIA]
SORRY, THERE'S A PROBLEM WITH YOUR CREDENTIALS. YOU'LL HAVE TO CHECK WITH THE SECURITY OFFICE.


IF CREDENTIALS COULDN'T BE SPOOFED, WE WOULD USE A MODERN APPROACH TO OLD-FASHIONED SOCIAL ENGINEERING. *GYGES ONE* COULD IDENTIFY ANYONE AT ARN WITH ISSUES TO BE EXPLOITED: MARITAL PROBLEMS, HEALTH OR FINANCIAL ISSUES.
A SECURITY GUARD WORKING OVERNIGHTS AND EARLY MORNINGS. LONELY, BITTER, A CUSTODY BATTLE DIDN'T GO HIS WAY ... SOMEONE WHO NEEDS SOMEONE TO TALK TO.


A DATING APP COULD CONNECT A LONELY GUARD WITH SOMEONE OF OUR CHOOSING, WITH PERIODIC'S HELP.
PETER?


THAT COULD **NEVER** HAPPEN. OUR SYSTEM DOESN'T TARGET PEOPLE LIKE THAT.
IT ALREADY DOES. YOU JUST DIDN'T REALIZE IT.


I CANT BELIEVE YOU WORK THERE! I HAVE A JOB INTERVIEW AT ARN TOMORROW.


STOP
SECURITY CHECK
HI PETER, LAST NIGHT WAS FUN!
I'M NOT SURE WHY, BUT I DONT SEE YOU ON THE VISITOR LIST ...
IT MUST BE A MISTAKE. I CAN LET YOU IN.


THANKS PETER!
SEE YOU, UM ... LATER?

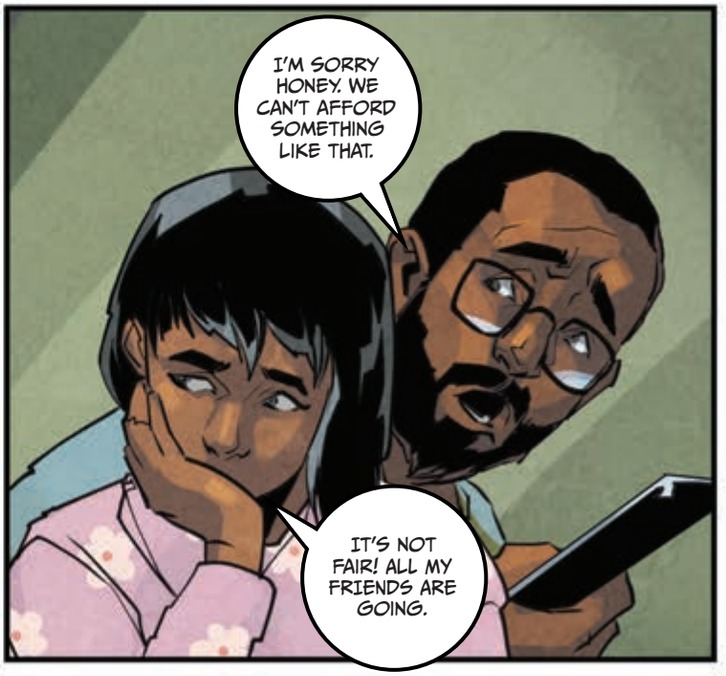

WAIT ... IS THIS REALLY A HYPOTHETICAL OR ... NO.
WE HOST THOSE DATING APPS TO HELP BRING PEOPLE TOGETHER, NOT TO MANIPULATE PEOPLE FOR ULTERIOR MOTIVES.


YOU NEVER CONSIDERED WHO **ELSE** COULD USE THIS DATA.
NOBLE INTENTIONS OR NOT, MANIPULATION IS MANIPULATION. ONCE YOU HAVE INFORMATION, IT CAN BE USED FOR PURPOSES THAT AREN'T DEFINED IN SOME QUAINT "TERMS OF SERVICE."
THIS IS ALL VERY INTERESTING, DISTURBING, EVEN, BUT WHY BRING THIS TO ME **NOW**? THERE'S AN INTERNATIONAL RESCUE EFFORT WE'RE TRYING TO H--


YOUR PATIENCE WILL BE REWARDED, I ASSURE YOU.
HERE'S ANOTHER QUESTION, RIDICULOUS ON THE SURFACE... HOW COULD A 13-YEAR-OLD GIRL'S LOVE OF HORSES DESTABILIZE AN INTERNATIONAL MINING AGREEMENT?
MACHINE-LEARNING ALGORITHMS FIND PATTERNS AND VULNERABILITIES THAT HUMANS MIGHT NOT.

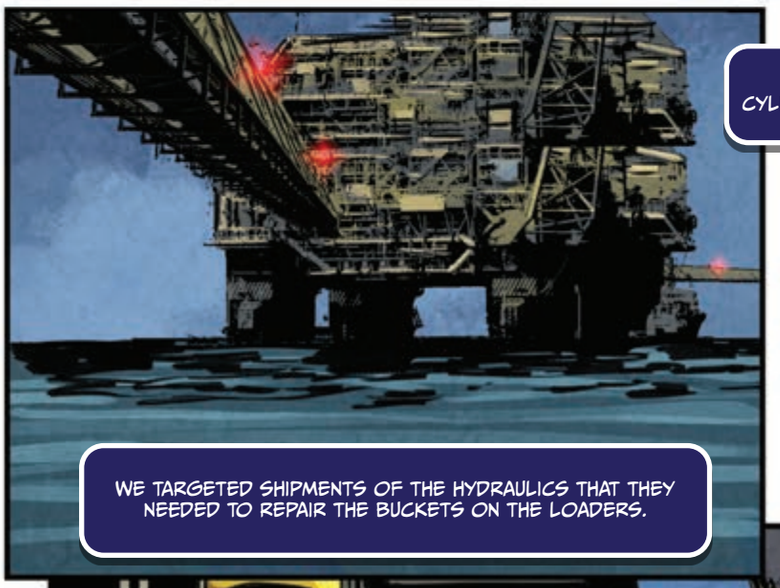

GREGORY SIMON, ENGINEER
[ARN MINING HEADQUARTERS, ATROPIA]


LOOK DADDY, LOOK AT THIS NEW RIDING SCHOOL. CAN I GO?


I'M SORRY HONEY. WE CAN'T AFFORD SOMETHING LIKE THAT.
IT'S NOT FAIR! ALL MY FRIENDS ARE GOING.


WE MADE SURE GREGORY SIMON STARTED SEEING POSTS ABOUT HIS DAUGHTER'S FRIENDS AND THEIR FAMILIES TOURING ONE OF THE BEST STABLES IN EUROPE.
SIMON **LOVED** HIS JOB ... AND HE WAS THE **ONLY** ENGINEER WHO UNDERSTOOD THE LEGACY SYSTEM AND HOW TO TRANSFER IT TO THE NEW ARN SYSTEM.
FOR YEARS HE HAD BEEN ASKING TO TRAIN NEW ENGINEERS ON THE OLDER CODE, BUT THE COMPANY ALWAYS SAID NO, ARGUING IT WAS TOO EXPENSIVE.
IT WAS EASY TO ARRANGE FOR A HEADHUNTER TO CONVINCE HIM TO CONSIDER LEAVING HIS JOB AT ARN.
YES, I GOT YOUR EMAIL. YOU WEREN'T KIDDING ABOUT THE SALARY.
Your Journey Awaits
WHEN A JOB OFFER CAME IN THAT MORE THAN **DOUBLED** HIS PAY, HE COULDN'T RESIST.
I'M TRULY SORRY SIR. BUT IT'S AN OPPORTUNITY I CAN'T PASS UP.
WE'LL MISS YOU, GREGORY. YOU'VE BEEN WITH US A LONG TIME.
SO HE GETS TO SEND HIS DAUGHTER TO HER DREAM SCHOOL BECAUSE SOMEONE ELSE RECOGNIZED HIS VALUE? THAT'S NICE, BUT WHAT'S YOUR POINT?
WELL, IT'S **NOT** THAT HE'S A GOOD DAD. IT'S THAT NOT PROTECTING INSTITUTIONAL KNOWLEDGE HAS CONSEQUENCES.
BECAUSE ARN AND THE ATROPIAN GOVERNMENT NEVER CONSIDERED THE NEED FOR REDUNDANCY. GREGORY SIMON'S SINGULAR KNOWLEDGE MADE HIM MORE IMPORTANT THAN **ANYONE** REALIZED. FROM REPLACEABLE COG TO INTEGRAL PART.
AS A RESULT, IF THE ARN PARTNERSHIP FAILS, THE ATROPIAN MINING COMPANIES ARE GOING TO HAVE TO GO IT **ALONE**.


OVER THE PAST FEW MONTHS WE'VE BEEN ERODING ARN'S SUPPLY CHAIN.


WE TARGETED SHIPMENTS OF THE HYDRAULICS THAT THEY NEEDED TO REPAIR THE BUCKETS ON THE LOADERS.


IT'S A **VERY** SPECIFIC CYLINDER AND CONTROL VALVE.
AND THEY MISSED IT WHEN OUR SUBSIDIARY COMPANY H&C TOOK A MAJOR STAKE IN THEIR PRIMARY PRODUCER.


THE RIG WORKERS COULDN'T MAINTAIN THEIR EQUIPMENT BUT WERE AFRAID TO ADMIT IT.
THEY LIED ABOUT IT, WHICH LED TO EVEN MORE EQUIPMENT FAILURES. AS A SAFETY FEATURE, THEIR SOFTWARE WOULD DISABLE ANY VEHICLES BEHIND ON REQUIRED MAINTENANCE.


THEY WANTED TO OVERRIDE THOSE SETTINGS, BUT THE LEASED TRACTOR PROVIDER REFUSED BECAUSE IT WOULD VOID THE WARRANTY.


THE SUPPLY CHAIN MANIPULATION SLOWED DOWN EVERYTHING. THEN WE STARTED ON THEIR LABOR RELATIONS. ARN NEVER HAD A GOOD RELATIONSHIP WITH THE LOCAL RIG WORKERS. DESPERATE, THE ARN ENGINEERS DECIDED A PRODUCTIVITY APP WOULD HELP GET THINGS BACK ON TRACK.
ARE YOU **KIDDING** ME? PRODUCTIVITY APPS ARE JUST ANOTHER WAY THE BOSSES CAN TRACK OUR EVERY MOVE ...
THEY ARE TRYING YO TURN US INTO ROBOTS TO KEEP UP WITH THEIR DEMANDS!
THEY THOUGHT THAT IF THEY JUST PAID PEOPLE ENOUGH, THEY COULD FIGHT UNIONIZATION, BUT IT TURNS OUT PEOPLE DON'T LIKE BEING TREATED LIKE ROBOTS.
WE ARE NOT ROBOTS
STOP
TRACKING ME
OUR DESTABILIZATION EFFORTS WEAKENED ARN AND LEFT THEM SHORTHANDED, WITH REDUNDANCY LACKING IN **MULTIPLE** AREAS.
I HAD SEEN REPORTS ON SOME OF THE PERSONNEL AND SUPPLY CHAIN ISSUES, BUT NO ONE WAS CONNECTING ...
THESE WERE **NEVER** HYPOTHETICALS, WERE THEY?
I KNEW YOU'D GET THERE EVENTUALLY.
ARN STAKED THEIR COMPANY'S FUTURE ON THE LUCRATIVE UNDERWATER MINING IN ATROPIAN WATERS. THEY'D ALREADY SHUT DOWN THEIR TERRESTRIAL MINING OPERATIONS, SO IF THEY DIDN'T MEET THEIR QUOTA ON A VERY SPECIFIC TIMELINE, THEY WERE IN **TROUBLE.**
THERE SEEMS TO BE A **LOT** OF EFFORT PUT INTO THIS ENDEAVOR. DID YOU HAVE SOMETHING TO DO WITH THE FAILURE TO FIND THAT SUB? THAT POOR CREW ...
WITH PERIODIC'S HELP, WE CREATED AN ENVIRONMENT THAT **DISCOURAGED** SUCCESS.

TO FULFILL THE MASTER PLAN, WE USED AI - AUGMENTED SOCIAL MEDIA POSTS AND ALGORITHMS TO DRIVE MESSAGING THAT THE DOWNED SUB POSED AN ENVIRONMENTAL RISK.

BUT THERE **WASN'T** ANY DANGER. THOSE BATTERIES CAN WITHSTAND--

WE KNOW. WE JUST NEEDED PEOPLE TO **THINK** THERE WAS A DANGER.

ANGELA SHEVCHENKO, INTELLIGENCE AGENT [ATROPIA]

AND EVEN THOUGH IT CAME FROM SECRET LEAKED FILES FROM AN INTELLIGENCE AGENT, IT WASN'T EVEN A TOP-SECRET LEAK ...

CHERNOBYL, KYIV OBLAST, UKRAINE 1986

WE CROSS-REFERENCED LISTS OF USERS ON YOUR PLATFORM WITH INDIVIDUALS WHO HAD ACCESS TO CLASSIFIED REPORTS ABOUT THE SUBMARINE.

WE FOUND ANGELA SHEVCHENKO, WHO GREW UP IN THE SHADOW OF THE CHERNOBYL DISASTER. BECAUSE HER GRANDFATHER HAD DIED AT CHERNOBYL, SHE WAS HIGHLY SUSPICIOUS OF ALL CLAIMS OF "SAFE" NUCLEAR POWER.

SHE BELIEVED THE PUBLIC SHOULD KNOW "THE TRUTH" AND NOT GET CAUGHT OFF GUARD THE WAY HER FAMILY DID.

Nuclear Sub Lost!

Public Private Failure

What went wro

Fall Out Panic

Featured

Should we start testing the children?

Featured Sections

/articles/

Officials knew that nuclear sub was not sea worthy.

Officials knew that a nuclear submarine was not seaworthy but still allowed it to operate. It would be a serious breach of safety protocols and could potentially endanger the crew and the environment.

By Alexandra Arsenault

www.tragedy.ww

LIVE

www.leakednews.xi

LEAKED DOC

Crew Feared Dead.

Leaked doc proves that nuclear sub should not have been allowed to launch

The News.

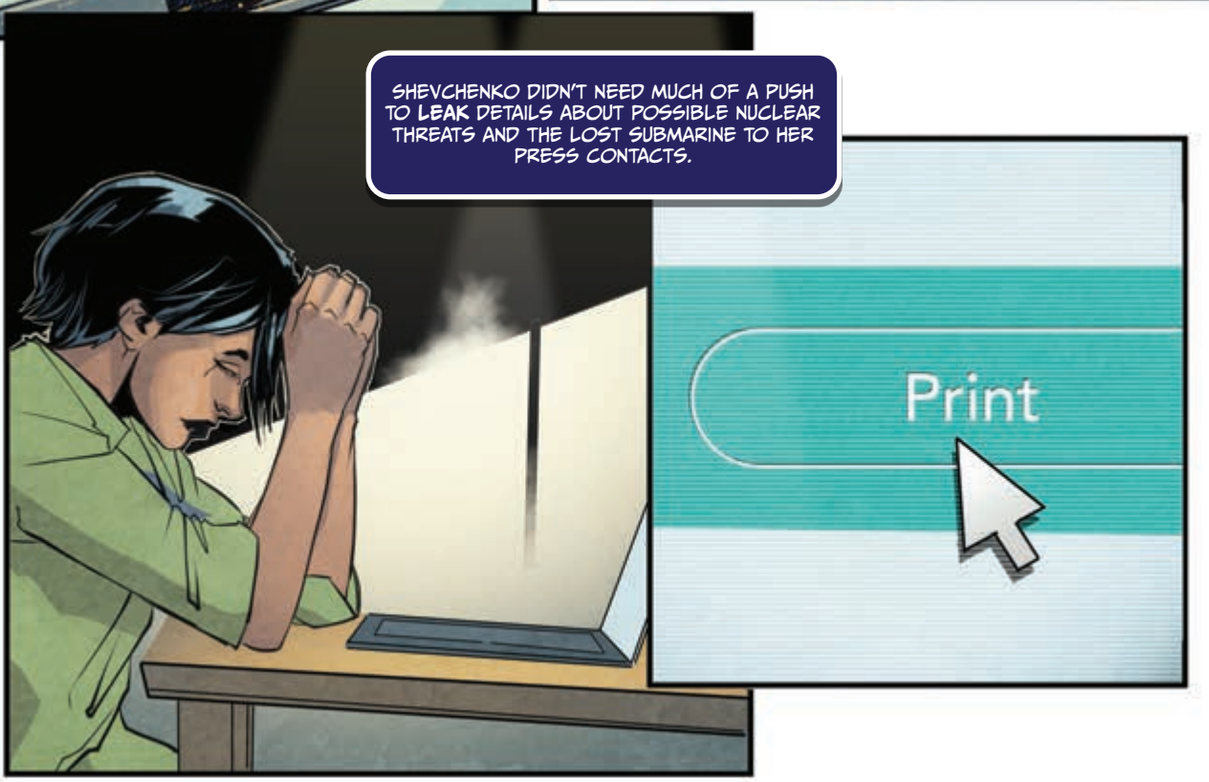
2030

Contaminated fish showing up at local fish markets.


PERIODIC USERS HAVE BEEN BUILDING THEIR PROFILES SINCE THEY WERE CHILDREN. EVERYTHING THEY SAW, THEY LIKED, THEY SHARED.
SOCIALIZATION ALGORITHMS CAN TARGET THE THINGS THAT ARE LIKELY TO PUSH AN INDIVIDUAL'S BUTTONS.


CHORNOBY
OUT PANIC:
WE'VE BEEN ABLE TO CREATE INCREDIBLE PREDICTIVE MODELS FOR WHEN, WHERE, AND WHY PEOPLE WILL TUNE OUT CERTAIN MESSAGES AND WHEN THEY'LL PAY ATTENTION TO OTHERS ...


BUT SIR, WHAT ABOUT THE RUMORS I'M SEEING ABOUT THIS BEING A POTENTIAL NUCLEAR DISASTER. IF PEOPLE ARE GOING TO DIE FROM THE NUCLEAR MELTDOWN, SHOULDN'T WE WARN SOMEONE?
I PROMISE THOSE THREATS HAVE BEEN EVALUATED. YOU'VE GOT TO TRUST THAT THE APPROPRIATE AGENCIES HAVE THIS HANDLED.


SHEVCHENKO DIDN'T NEED MUCH OF A PUSH TO LEAK DETAILS ABOUT POSSIBLE NUCLEAR THREATS AND THE LOST SUBMARINE TO HER PRESS CONTACTS.
Print


Legit Press:
INTELLIGENCE AGENT LEAKS CLASSIFIED REPORT ABOUT LOST NUCLEAR SUB.
>> AS SEEN ON: FRINGENEWS.COM
THE FRINGE PRESS RAN WITH HER LEAKS. THEN IT SPREAD TO MAINSTREAM MEDIA.
ATROPIANS STUNNED BY THE DOCUMENT LEAK FROM AN INTELLIGENCE AGENT WHO HAD ACCESS TO CLASSIFIED REPORTS...
NO.
NUCLEAR SUB LOST
Sub Gate:
WHO KNEW? WHO LIED?
RADIO SILENCE - CREW FEARED DEAD
HOW MANY WILL DIE FROM THE NUCLEAR SUB DISASTER?


THE LEAKS GOT AGENT SHEVCHENKO ARRESTED, WHICH MADE THE INFORMATION SEEM MORE LEGITIMATE.
LEAKING INFORMATION WAS UNFORGIVABLE, WHETHER IT WAS ACCURATE OR NOT. SHE WILL SPEND YEARS IN JAIL CONVINCED SHE DID RIGHT, NOT CARING ABOUT THE HARM SHE CAUSED... OR REALIZING THAT SHE WAS NEVER THE ONE MAKING THE DECISIONS.

THE DEVIL IS IN THE DATA: PUBLICLY AVAILABLE INFORMATION AND THE RISKS TO FORCE PROTECTION AND READINESS

MAJ Joe Littell, MAJ Maggie Smith, and MAJ Nick Starck

Originally published as part of the Army Cyber Institute's/Modern War Institute's Competition in Cyber Project [https://mwi.usma.edu]
09.20.2022

In the early 2010s, mass protests and riots ripped through the Middle East and North Africa as the Arab Spring gathered support. Longtime authoritarians like Zine El Abidine Ben Ali of Tunisia, Hosni Mubarak of Egypt, Muammar Gaddafi of Libya, and Bashar al-Assad of Syria all struggled to contain the groundswell after decades of rule. The rest of the world watched the human rights atrocities broadcast live on social media directly from those living through it instead of from traditional media institutions or foreign correspondents. The ubiquity of cellular phones and social media had democratized media production, and the world had a front-row seat to revolution and upheaval.

The shift in information sharing, from formal media to informal social media, was accompanied by a shift in who could act on that information. Fearless netizens began collecting images from Twitter and videos from YouTube and comparing them with Google Street View and other publicly available reverse image search tools. People like Eliot Higgins, founder of open-source investigation and journalism outfit Bellingcat, cut their teeth on the media coming out of the Arab Spring and the bloody civil wars that followed. Most efforts were focused on doing good, and an entire human rights cottage industry sprung up around the new data sources and the analytic groups documenting violence as it happened all over the world. Many believed that we were finally seeing the promised societal benefits of innovative technologies and that the near-constant data collection and advanced analytic techniques, like artificial intelligence and machine-learning algorithms, would really change the world.

However, as with all technology, there is also a dark side to the big data explosion that poses significant risks to privacy and national security. The deliberate corporate collection of personal data, often referred to as the modern surveillance economy, has a singular goal—to shape consumer behavior. Put more bluntly, producers want consumers to buy more, and big data allows corporations to know what individuals like and what makes them click "purchase." But consumer data is not just available to corporate entities, in fact, anyone with the right amount of money can buy it in droves—nation-state adversaries can purchase data pools of publicly available information (PAI) about U.S. consumers, their likes and dislikes, for analysis and influence, which is something that private marketing firms and authoritarian regimes have been quick to exploit, and democratic governments have been slow to prevent.

The United States is still struggling to understand the national security risk posed by publicly available information. The 2018 Joint Concept for Operating in the Information Environment took steps to describe the information environment as consisting of three dimensions: the data-centric information dimension, the human-centric cognitive dimension, and the real-world physical dimension. Further, in 2022, the amended National Defense Authorization Act directed elements of

DOD to assess the challenges of operating in the presence of "ubiquitous technical surveillance." Efforts to respond to these challenges are ongoing. Among the notable endeavors are the Army's Information Advantage concept and the recent release of the Marine Corps Doctrinal Publication 8, Information. However, in the case of the Army's Information Advantage concept, the operationally focused efforts are overly narrow and fail to adequately address the scope of the challenges.

What DOD must acknowledge first is the fundamental source of risk to the U.S. military from the information environment, namely the vast amounts of data collected and sold on U.S. service members. And our adversaries can (and do) use the commercial data economy to target U.S. service members and their families, and to pollute the information environment to diminish operational effectiveness. To adequately respond to this concerning shift in the operational environment, it is necessary to understand the categories of risk created by the collection of U.S. service member data to help prioritize risk decisions and to improve the military's technical understanding of how the surveillance economy works. To frame the problem, we need to begin conceiving of actions in the data-centric information dimension as creating risk in the cognitive and physical dimensions of the information environment.

"Nation-state adversaries can purchase data pools of publicly available information (PAI) about U.S. consumers, their likes and dislikes, for analysis and influence, which is something that private marketing firms and authoritarian regimes have been quick to exploit, and democratic governments have been slow to prevent."

Cognitive Dimension Risks

The cognitive dimension of the information environment is defined by how humans understand, react to, and interact with the world based on the information they are exposed to. By extension, for the military, cognitive risks are any alteration to the perception and behavior of some number of individuals in a manner that will negatively impact a commander's ability to accomplish a mission or national priorities. Shaping perception and influencing behavior are two tasks that the modern surveillance economy is designed to facilitate and, when data on U.S. persons is purchased, can enable adversaries to shape and influence how Americans think.

Like traditional operational risks, cognitive risks result from both adversary and friendly actions, and can manifest both internally and externally to an organization. Adversaries can use surveillance technologies to efficiently target key audiences, like service members, government employees, or even their families with mis- and disinformation. Friendly actions (and inactions) can

also create cognitive risks by eroding trust in the government and military, shaping fundamental behaviors like volunteering to enlist, and creating fodder for adversary information operations. Adversary operations may also target key military support constituencies and create cognitive risks to military operations, recruitment, and retention. For example, both Russia and Ukraine have leveraged these technologies during their ongoing conflict, creating cognitive risks from Russians calling and texting Ukrainian soldiers on the front lines to Ukrainians calling the mothers of Russian soldiers captured during the conflict. However, importantly—and critically for the U.S. military—cognitive risks are not constrained to periods of armed conflict or deployment, and in many cases are more prevalent and impactful during normal garrison operations and are often external to any conflict.

Actualized examples of cognitive risks are numerous. Within the U.S. population, they include mobilizing protestors, inflaming opinions on both sides of contentious social issues, and deepening issue divergence among ideologically opposed groups. These examples show how surveillance technologies generate cognitive risk and may present a real threat during competition and crisis. Cognitive risks—with even the most tenuous connection to "traditional" Army missions—can pose some of the most serious risks to the force given their ability to fester and grow over time, erode trust, and disrupt cohesion within a unit and among key support constituencies. Ignoring or dismissing cognitive risks as falling outside of the Army's mandate or claiming that cognitive risks are an individual's responsibility is obtuse and potentially catastrophic to our ability to operate on the modern battlefield.

Protecting any population against cognitive risks is a delicate balance—particularly in a democracy. In the United States, First Amendment protections and an individual's freedom to access information are two characteristics of our democracy that malign actors regularly exploit and abuse to gain access to U.S. service members' cognition. But by recognizing that cognitive risks exist and that they have the potential to impact mission success, we also create opportunities to act thoughtfully, to detect, assess, and make risk decisions to drive mitigation efforts without having to consider the politics of the content being consumed. And effective risk categorization enables a better understanding of the threats to the force and will allow commanders to balance the informational freedoms we value with the need to defend the cognitive dimension.

Physical Dimension Risks

The most direct and obvious personal data risks to military forces occur in the physical world. Namely, publicly available information can be—and is—used for kinetic targeting. U.S. government officials and service members, both at home and abroad, generate a lot of PAI as they go about their daily routines, revealing location data, travel data, purchasing data, and more. The concern for the military is how that personal data can be used to target individuals for kinetic strikes on the battlefield. The ongoing conflict in Ukraine is an example of how PAI can be used to identify unsecure cell phones and enable location triangulation for kinetic attacks on conventional forces. In fact, at least one PAI-enabled kinetic strike has led to the death of a Russian general officer and Russia also leveraged PAI against Ukraine from 2014 to 2016.

However, the physical risk from PAI is not limited to location data. Imagery, from social media and official state sources, for example, can be compared to the robust database of landscapes found in programs like Google Earth to pinpoint operationally relevant locations—a technique that led to the loss of a Russian naval vessel. The U.S. military has also used similar targeting

practices to direct drone strikes against ISIS targets using selfies and social media. Within DOD, therefore, commanders intuitively understand the seriousness of the tasks conducted to obfuscate their formations in time and space and the danger posed by inadvertent exposure. But increasingly, risks are coming from obscure places—like the 2018 example of how the exercise app Strava allowed for the identification of sensitive military locations through its Strava Heat Map feature. DOD responded with a new policy—nine months after the risk was identified—that banned the use of geolocation app features in deployed settings.

"Without fully understanding how these data systems impact military operational effectiveness, the United States sets itself at a strategic disadvantage."

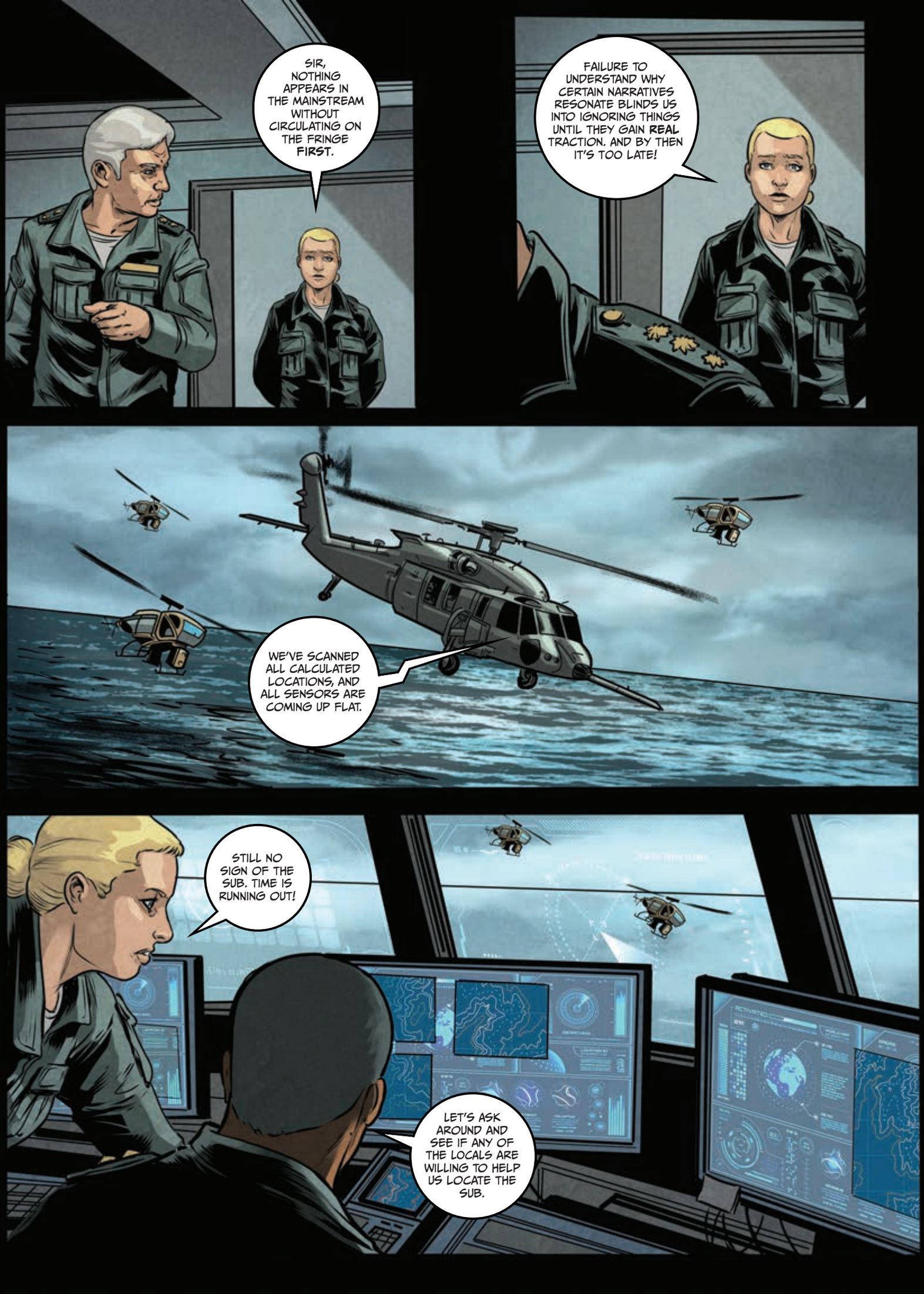
The DOD's response to the Strava incident has since expanded to other technologies, including the Army's outright ban on cellphones for deploying troops, citing operational security and cybersecurity concerns. And even though the general awareness of physical risks created by data is growing (and is a good thing), an outright ban on certain technologies is not a sustainable risk mitigation strategy. The prohibition of personal devices is simultaneously too narrow and too broad and fails to strike an appropriate balance between necessary modernization and operational security. By focusing on conflict zones and deployed settings, DOD misses the physical risks those devices and their resulting PAI generate. And by banning devices and apps, DOD is inadvertently generating physical risks because typical patterns of life are suddenly disrupted when those devices and apps go dark—the absence of digital data and signatures is also observable and could direct adversary attention to units and personnel heading overseas or conducting field training exercises. A more deliberate approach to assessing the risks in open-source data and how actions in the information environment create signals for adversaries is needed to achieve sustainable and substantive mitigation strategies.

The commercialization of personal data and the practices of commercial data brokers have enabled companies and our adversaries to accumulate vast amounts of knowledge on U.S. persons, including our service members. Without fully understanding how these data systems impact military operational effectiveness, the United States sets itself at a strategic disadvantage. Understanding the vulnerabilities created by the commercial surveillance economy and identifying the associated risks is necessary for commanders to make informed risk decisions. While the wholesale removal of risk is not possible, a careful examination of risk can shape policy, open pathways for technical mitigation strategies, and define best data hygiene practices.

DOD's role in this effort should focus on gaining and maintaining operational security, which demands a layered approach that prescribes taking measured action at each echelon—individual, unit, and institutional—and prioritizing actions through a deliberate assessment of the operational risk. Importantly, any strategy must include individual education, institutional investment, and the implementation of privacy-preserving technologies. These efforts should mirror the approach taken toward cybersecurity, where DOD has acted to both secure its own networks and invest in initiatives like the Home Use Program to make security (or, in this case, privacy) more accessible to its service members. Ultimately, without a layered approach to addressing the risks generated by publicly available information and the surveillance economy, DOD will fail to protect its most valuable asset—its people—and will not be prepared to fight on the modern battlefield.

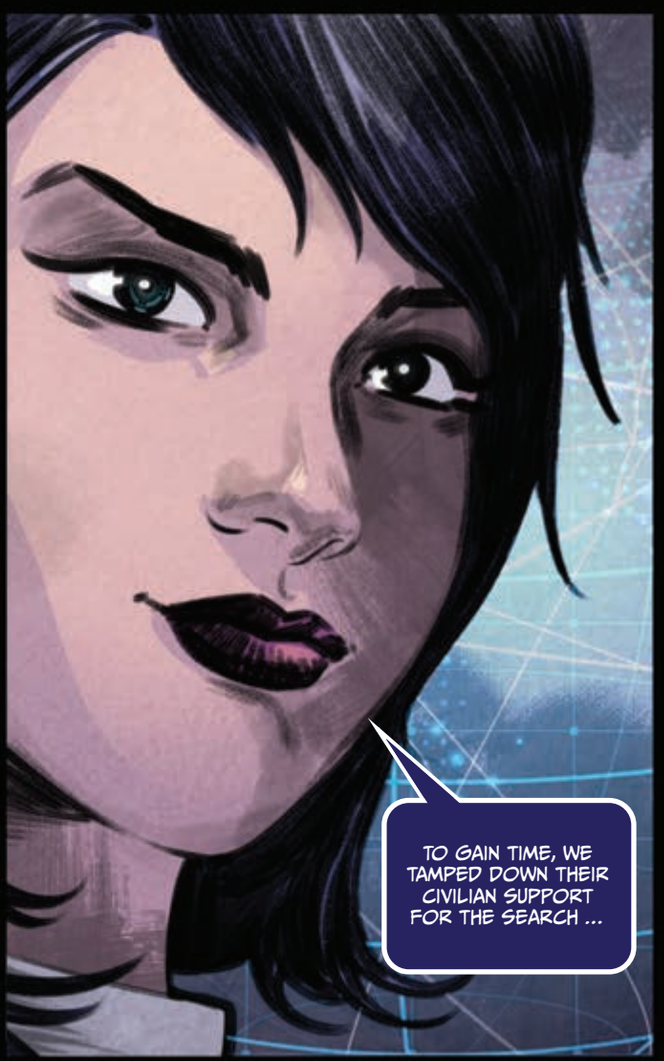

MY COUNTRY HAS WANTED TO BUILD A BETTER RELATIONSHIP WITH ATROPIA FOR **YEARS**, AND CREATING A MORE HOSTILE ENVIRONMENT FOR ARN PROVED TO BE THE CRUCIAL STEP.
ATROPIAN AUTHORITIES REACHED OUT TO OUR **DONOVIAN** NAVY TO LOCATE THE MISSING SUBMARINE.
EVEN THE LOCAL FISHING FLEETS WERE ACTIVATED TO AID IN THE SEARCH.
WHO DIES? WHO PAYS?
FOREIGNERS OUT!
NGOs
PROTESTS ERUPTED ACROSS ATROPIA, CALLING FOR ALL FOREIGN PRESENCE OUT OF THEIR SHARED WATERS FOR FEAR OF CHEMICAL POLLUTION.
FOREIGN NGOS WERE REPORTEDLY ATTACKED BY PROTESTORS WHEN TRYING TO ASSESS THE LEVEL OF POLLUTION FOR CLEANUP.
IN WHAT CAME AS A SURPRISE TO SOME, DONOVIA MOBILIZED ITS **ENTIRE** MILITARY IN A RESCUE MISSION ... THOUGH ONE WITH A **SECONDARY** PURPOSE.
WHILE OUR GOAL IS TO LOCATE THE MISSING SUBMARINE AND RESCUE ANY SURVIVORS, WE MUST ALSO DISCOVER WHAT OTHER SECRET ACTIVITIES ARN INDUSTRIES HAS BEEN ENGAGING IN IN THE ATROPIAN SEA. OUR SOVEREIGNTY IS NOT FOR SALE!


Meanwhile, because of the rising tensions in the region, an ARN-backed rescue team was dispatched to locate the lost sub and its crew. Time was essential.
The whole situation is a **mess** because of this lost sub!
Local protests are getting more heated. Now the Donovian navy is on the way.
We need to find this submarine and dismantle this developing alliance between Atropia and Donovia.
Sir, we need to pay attention to the narratives emerging from the fringe channels.
There are rumors on the fringe that this is a false flag and that the West is using it as a cover to disrupt Atropian & Donovian mining operations.
We're not going to react to some unsubstantiated message on the dark web. We can't play whack-a-mole with every crazy idea on the internet!!


SIR, NOTHING APPEARS IN THE MAINSTREAM WITHOUT CIRCULATING ON THE FRINGE **FIRST**.
FAILURE TO UNDERSTAND WHY CERTAIN NARRATIVES RESONATE BLINDS US INTO IGNORING THINGS UNTIL THEY GAIN **REAL** TRACTION. AND BY THEN IT'S TOO LATE!
WE'VE SCANNED ALL CALCULATED LOCATIONS, AND ALL SENSORS ARE COMING UP FLAT.
STILL NO SIGN OF THE SUB. TIME IS RUNNING OUT!
LET'S ASK AROUND AND SEE IF ANY OF THE LOCALS ARE WILLING TO HELP US LOCATE THE SUB.


WE DIDN'T HAVE AS MUCH OF A HEAD START AS WE WOULD HAVE LIKED. WE NEEDED TO FIND THE SUB BEFORE ARN'S RESCUE AND RECOVERY TEAM.


USING PRIVATE SIGNAL MONITORING, OUR SIGNALS INTELLIGENCE PICKED UP THEIR LOCATION.
WE HAVE COORDINATES.


TO GAIN TIME, WE TAMPED DOWN THEIR CIVILIAN SUPPORT FOR THE SEARCH ...


MALIK BITAR, FISHING BOAT CAPTAIN [ATROPIAN SEA]
WE KNEW ATROPIA WOULD HAVE NO CHOICE BUT TO REACH OUT TO THE DONOVIAN FISHING FLEET FOR HELP. SO WE HAD TO RATCHET UP ANTI-ARN SENTIMENT ... AND QUICKLY.
...WE COLLECTED DATA FROM THIRD-PARTY MARKETERS AND HAD A FULL PICTURE OF THE LOCAL FISHING FLEET'S BACKGROUNDS AND CURRENT LOCATIONS.
MANY OF THE LOCAL FISHERMEN HAVE AT LEAST MILD HOSTILITY TOWARDS ARN AND THE WEST.
ATTENTION ALL VESSELS IN THE VICINITY ...
MARITIME ALERT
TAKING THEM OUT OF THE RECOVERY OPERATION WAS A HIGH PRIORITY, SO WE AMPLIFIED TOPICS THAT TRIGGERED LOCALIZED ANGER AND FRUSTRATION.
THE MARITIME NETWORK
MORE
MORE
MORE
ALERT
DISMISS
WHY SHOULD I HELP? I HAVE TOO MUCH TO DO ALREADY ...


WAIT. THE SUB WAS **FOUND**? HOW HAS THAT BEEN KEPT QUIET?
YOU STILL DON'T UNDERSTAND THE INFLUENCE WE HAVE HERE, DO YOU?
WE HAD REGAINED OUR ADVANTAGE AND GOT TO THE SUB FIRST ...
I REPEAT, WE HAVE LOCATED THE MISSING SUB INTACT. IT APPEARS THE CREW HAS ESCAPED IN LIFE PODS.
...BUT RETRIEVING THE CREW OURSELVES REMAINED CRITICAL TO OUR PLAN.

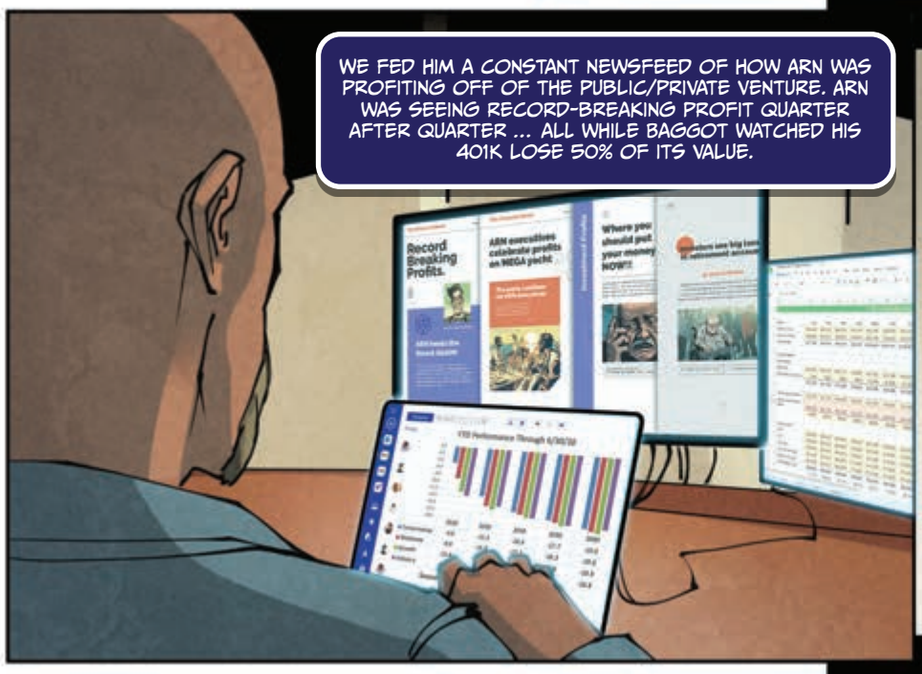
JEFF BAGGOTT, INTELLIGENCE OFFICER
[U.S. ALLIED BASE]

JEFF BAGGOTT, A WESTERN INTELLIGENCE OFFICER, UNKNOWINGLY GAVE US THE LITTLE EXTRA TIME WE NEEDED TO PULL UP THE SUB AND RESCUE THE MISSING CREW.

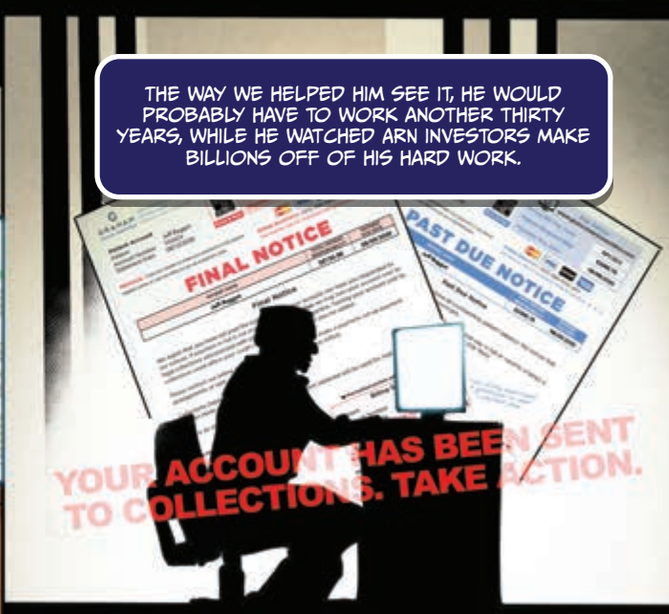
BAGGOTT'S ASSIGNMENT WAS TO FIND THE SUBMARINE.

HE HAD JUST RECEIVED HIS THIRTY-YEAR PIN FOR CONTINUOUS SERVICE, BUT HE WAS HAVING FINANCIAL TROUBLES AT HOME, FIGHTING WITH HIS SPOUSE ...

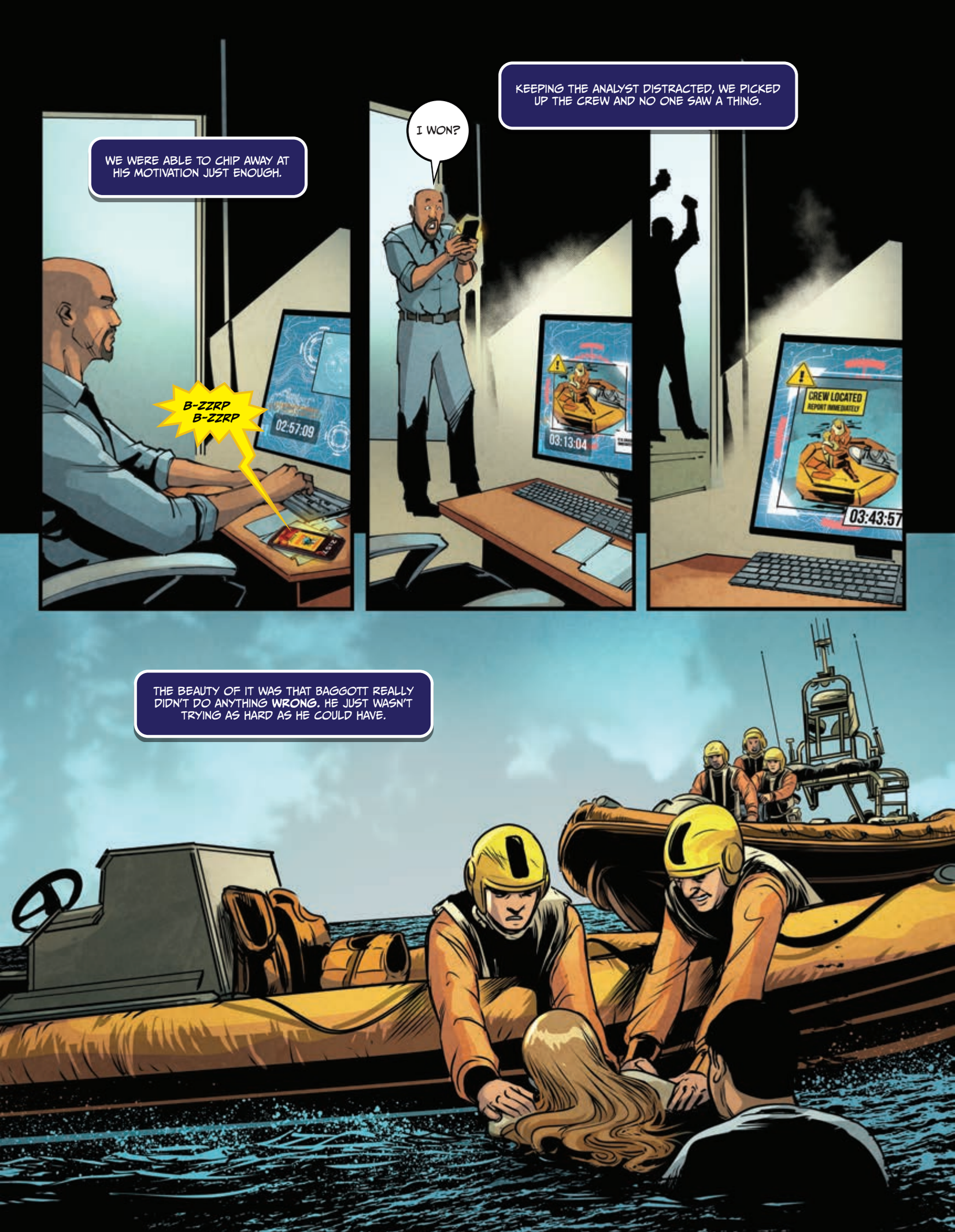
WE FED HIM A CONSTANT NEWSFEED OF HOW ARN WAS PROFITING OFF OF THE PUBLIC/PRIVATE VENTURE. ARN WAS SEEING RECORD-BREAKING PROFIT QUARTER AFTER QUARTER ... ALL WHILE BAGGOT WATCHED HIS 401K LOSE 50% OF ITS VALUE.

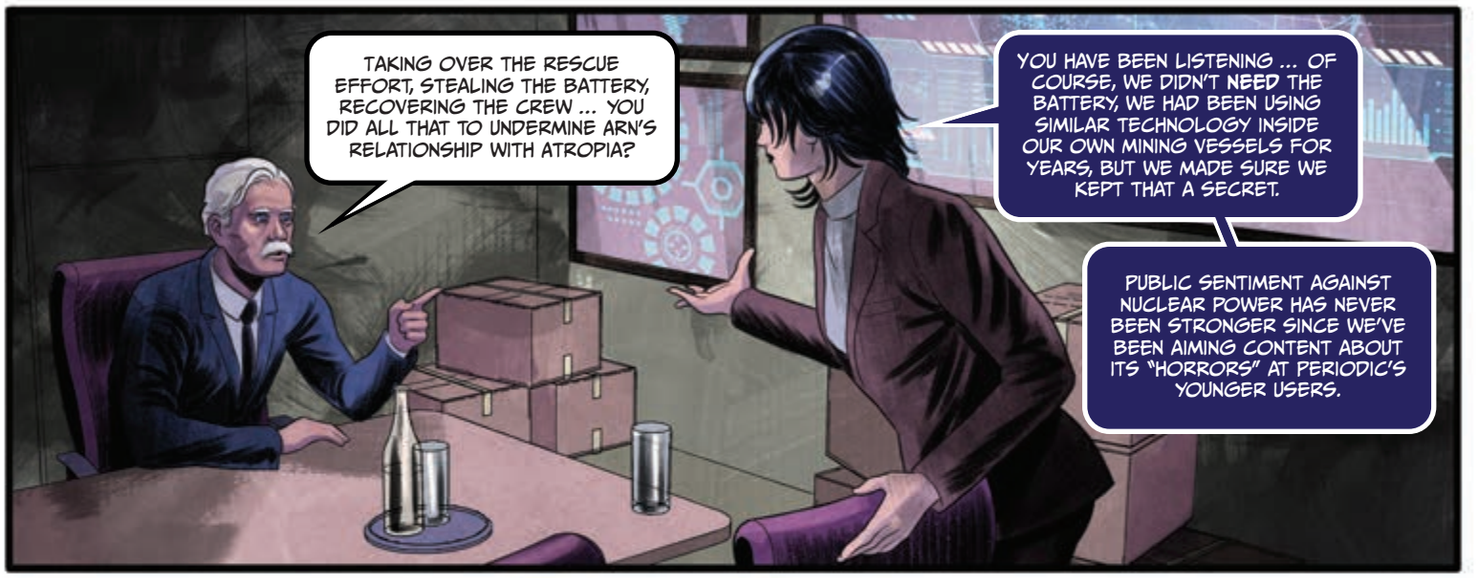


THE WAY WE HELPED HIM SEE IT, HE WOULD PROBABLY HAVE TO WORK ANOTHER THIRTY YEARS, WHILE HE WATCHED ARN INVESTORS MAKE BILLIONS OFF OF HIS HARD WORK.



WE KNEW THE ANALYST WAS FIGHTING WITH HIS WIFE, HAD FINANCIAL WORRIES, AND WAS NOW SUSPICIOUS OF ARN.

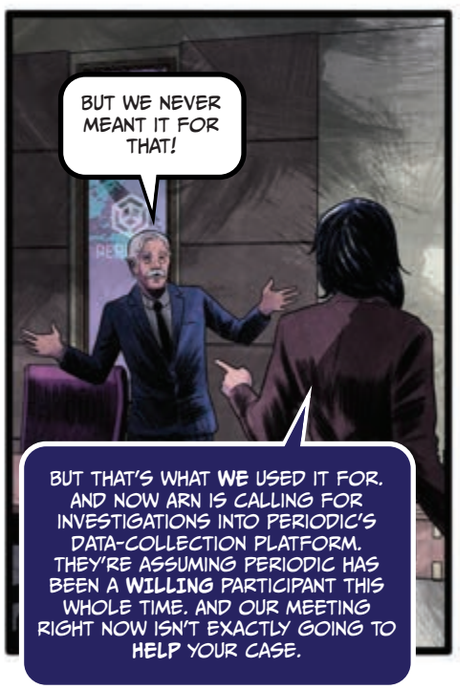

WE WERE ABLE TO CHIP AWAY AT HIS MOTIVATION JUST ENOUGH.
B-ZZRP B-ZZRP
02:57:09
I WON?
03:13:04
KEEPING THE ANALYST DISTRACTED, WE PICKED UP THE CREW AND NO ONE SAW A THING.
CREW LOCATED
REPORT IMMEDIATELY
03:43:57
THE BEAUTY OF IT WAS THAT BAGGOTT REALLY DIDN'T DO ANYTHING **WRONG.** HE JUST WASN'T TRYING AS HARD AS HE COULD HAVE.


TAKING OVER THE RESCUE EFFORT, STEALING THE BATTERY, RECOVERING THE CREW ... YOU DID ALL THAT TO UNDERMINE ARN'S RELATIONSHIP WITH ATROPIA?
YOU HAVE BEEN LISTENING ... OF COURSE, WE DIDN'T **NEED** THE BATTERY, WE HAD BEEN USING SIMILAR TECHNOLOGY INSIDE OUR OWN MINING VESSELS FOR YEARS, BUT WE MADE SURE WE KEPT THAT A SECRET.
PUBLIC SENTIMENT AGAINST NUCLEAR POWER HAS NEVER BEEN STRONGER SINCE WE'VE BEEN AIMING CONTENT ABOUT ITS "HORRORS" AT PERIODIC'S YOUNGER USERS.


WHY THE CREW THEN?
INSURANCE. IF ANYTHING WENT WRONG WITH THE TRANSFER OF POWER FROM ARN TO US, THE CREW WOULD HAVE BEEN JUST ANOTHER BARGAINING CHIP.


I SEE.
DO YOU?


THESE NEW TOYS I MENTIONED – A SUITE OF AI TOOLS TO TARGET ANYONE, ANYWHERE – ARE ALL FUELED BY THE DATA MINED FROM THE PERIODIC PLATFORM.


BUT WE NEVER MEANT IT FOR THAT!
BUT THAT'S WHAT **WE** USED IT FOR. AND NOW ARN IS CALLING FOR INVESTIGATIONS INTO PERIODIC'S DATA-COLLECTION PLATFORM. THEY'RE ASSUMING PERIODIC HAS BEEN A **WILLING** PARTICIPANT THIS WHOLE TIME. AND OUR MEETING RIGHT NOW ISN'T EXACTLY GOING TO **HELP** YOUR CASE.


BUT ... YOU CAN'T ...
IT'S ALREADY BEEN DONE. SOME OF OUR ACTIONS DURING THIS OPERATION HAVE BEEN DETECTED. EUROPOL IS PREPARING TO LAUNCH A PROBE OF PERIODIC AS AGENTS OF THE DONOVIAN STATE. I CAN MAKE SURE THEIR INVESTIGATION GOES **NOWHERE.**


AFTER ALL, WE MUST BE MORE THAN JUST BUSINESS PARTNERS NOW.
END.

AFTERWORD:

JUSTIN SHERMAN
SENIOR FELLOW AT DUKE UNIVERSITY'S SANFORD SCHOOL OF PUBLIC POLICY,
WHERE HE RUNS ITS DATA BROKERAGE RESEARCH PROJECT.

When most of us visit a website or use a mobile app, we know the website or app is, at some level, collecting information about us. Facebook and Twitter might gather data on our scrolls and clicks. Yelp or our local restaurant website might collect data on our food orders and searches. Even dating apps might collect data on our swipes and preferences, and GPS apps will collect data on the places we visit and when we visit them.

These are all companies we interact with directly. But what most people don't realize is that once an app or website has users' data, it often shares that information widely. For instance, apps might send users' data to advertisers, who receive information about those people's ages, locations, and smartphone activity. Another prominent part of this landscape is data brokers—companies that collect, infer and aggregate consumers' data, then sell, license, or share it for profit.

Data brokerage is a multi-billion-dollar, virtually unregulated industry in the United States encompassing thousands of companies. Data that people assume is closely held by a single website, app, or company—including data on politics, entertainment, location, and health—is often transmitted, analyzed, and monetized far beyond that one destination, all for the purposes of making a profit. It's all about collecting, aggregating, analyzing, buying, selling, and sharing data.

Research conducted at Duke University's Sanford School of Public Policy has shown that data brokers sell individuals' most sensitive information on the open market. This includes Americans' demographic information, such as race, religion, sexual orientation, income status, marital status, and number of children in the home; political preferences and beliefs, such as party membership, favorite candidates, and political causes of interest; health and mental health conditions, such as ailment and prescription information; and whereabouts and real-time locations.

Data brokers also advertise data on specific groups of Americans, including students, workers, first responders, elderly Americans, people with Alzheimer's, current and former U.S. government employees, and current and former members of the U.S. military. Some of the data is more "aggregated," meaning the datasets do not name specific people but provide overall analytics on the underlying information. Many other datasets, though, are clearly linked to specific people—and you can purchase these lists of attributes alongside Americans' names, emails, phone numbers, and home addresses. The most unbelievable part is that it's all legal. Because of gaps in U.S. privacy law, it's legal to acquire and then sell this sensitive data on Americans, even where it concerns data points like race, religion, marital status, sexual orientation, political affiliation, and geolocation.

"BECAUSE OF GAPS IN U.S. PRIVACY LAW, IT'S LEGAL TO ACQUIRE AND THEN SELL THIS SENSITIVE DATA ON AMERICANS, EVEN WHERE IT CONCERNS DATA POINTS LIKE RACE, RELIGION, MARITAL STATUS, SEXUAL ORIENTATION, POLITICAL AFFILIATION, AND GEOLOCATION.

The data brokerage ecosystem poses numerous risks to civil rights, consumer privacy, personal safety, and national security. Data brokers gathering and then selling data on military personnel poses a major risk to national security.

Foreign governments already collect data on U.S. citizens to enhance their intelligence operations, military posturing, and diplomacy. The Chinese government's 2015 hack of the U.S. Office of Personnel Management is an infamous example, where Chinese military officers stole data on over 22 million Americans who presently or previously worked for the U.S. government. But the list goes on: for instance, the Washington Post has reported on the Chinese government scraping open data overseas to target foreigners—and on a small Chinese company collecting millions of social media data points on "foreign political, military and business figures, details about countries' infrastructure and military deployments, and public opinion analysis." Hacking efforts by governments and criminal affiliates in Russia, Iran, North Korea, and elsewhere are likewise well-documented. Foreign actors can use this data to profile, target, or surveil Americans—and even to run cyber operations or intelligence operations.

All Americans' data is vulnerable to exposure, purchase, or theft through the data brokerage ecosystem. With military personnel, the risks to national security are clearer and more acute. Foreign citizens, companies, and governments can—under the current U.S. legal and regulatory system—entirely legally purchase highly sensitive data on Americans from U.S. companies, who are not constrained in brokering data to foreign actors. Perhaps more likely, foreign actors could also hack into data brokers and steal information that is dangerously collected, aggregated, and pre-packaged. This could include data such as where servicemembers are stationed, what entertainment and media members of the military consume, or the political interests of veterans in a Midwestern city. It could also include larger datasets that encompass military personnel as a subset, such as lists of gambling addicts, people suffering from

depression, or individuals with low credit scores (all of which are available on the open market). The data sold is remarkable in breadth and depth.

All of this data could be exploited for bribery, blackmail, routine intelligence collection, and much worse. For example, in one tragic 2020 case, an angry and violent lawyer found a federal judge's personal information online, went to her home while impersonating a delivery driver, and shot and wounded her husband and shot and killed her 20-year-old son. In many other cases each year, abusive individuals acquire data on people's whereabouts to track them down and stalk, harass, intimidate, and even physically harm them. Where national security is concerned, the availability of location data creates risks to the military as well—when malicious actors can buy data at low cost (single profiles on a "people search website" can cost $20) and relatively easily (plenty of data brokers do not appear to adequately vet their customers). Data brokers' ability to aggregate data and then "infer" data points that were never explicitly handed over, such as income level and sexual orientation, means they can be a more attractive and unique data source for malicious individuals.

Thankfully, the U.S. has the opportunity to build a comprehensive approach to data privacy and security—including banning the sale of data in certain sensitive areas, such as location data and health data. There is growing recognition in Congress of data brokerage, privacy harms, and risks to national security. The Protecting Military Service Members' Data Act would prevent data brokers from selling lists of military personnel to China, Russia, Iran, North Korea, and other adversarial nations. The White House's June 2021 executive order on Protecting Americans' Sensitive Data from Foreign Adversaries likewise recognized that "foreign adversary access to large repositories of United States persons' data also represents a significant risk." Nonetheless, Congress needs to focus more attention on regulating data brokers. That should include a focus on the ongoing sale of data, including data clearly linked to individuals, pertaining to military service members. For their part, service members can start by better educating themselves about the data brokerage ecosystem and the other ways that data collection, analysis, and targeting impacts them—such as by reading research from the Federal Trade Commission, Senate Commerce, Science, and Transportation Committee, World Privacy Forum, and our team at Duke's Sanford School of Public Policy.

> **"FOREIGN ACTORS CAN USE THIS DATA TO PROFILE, TARGET, OR SURVEIL AMERICANS—AND EVEN TO RUN CYBER OPERATIONS OR INTELLIGENCE OPERATIONS.**

If the U.S. is going to truly push for a more comprehensive data privacy and security model, including protecting national security, the military can play a key role in drawing attention to the risks.

INTRODUCTION FOOTNOTES:

*Facebook also owns Instagram, Oculus, and WhatsApp.

1. Bryan Sparling, "The Zhenhua Leak, IOS 14 and National Security.," LinkedIn, September 24, 2020, https://www.linkedin.com/pulse/zhenhua-leak-ios-14-national-security-bryan-sparling.

2. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, 1st edition (Location?PublicAffairs, 2019).

3. Christopher Wylie, Mindf*ck: Cambridge Analytica and the Plot to Break America (New York: Random House, 2019); Brittany Kaiser, Targeted: The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again (Location?Harper, 2019); Sasha Issenberg, The Victory Lab: The Secret Science of Winning Campaigns, Reprint edition (New York: Broadway Books, 2013).

4. Zeynep Tufekci, Twitter and Tear Gas: The Power and Fragility of Networked Protest, Reprint edition (New Haven, CT: Yale University Press, 2018).

5. "Communications Decency Act," 47 U.S. Code § 230, accessed November 19, 2020, https://www.law.cornell.edu/uscode/text/47/230.

6. Facebook, "Case Study: Reaching Voters with Facebook Ads (Vote No on 8)" (Menlo Park, CA: Facebook for Government, Politics & Advocacy, July 2011), https://www.facebook.com/notes/us-politics-on-facebook/case-study-reaching-voters-with-facebook-ads-vote-no-on-8/10150257619200882.

7. Channel 4 News Investigations Team, "Revealed: Trump Campaign Strategy to Deter Millions of Black Americans from Voting in 2016," Channel 4 News, September 28, 2020, https://www.channel4.com/news/revealed-trump-campaign-strategy-to-deter-millions-of-black-americans-from-voting-in-2016.

8. Dan Patterson, "Trolls Are Spreading Conspiracy Theories That a US Army Reservist Is 'COVID-19 Patient Zero,' China Is Amplifying That Disinformation," CBS Evening News, April 30, 2020, online edition, https://www.cbsnews.com/news/coronavirus-patient-zero-china-trolls/.

CREATIVE INDEX

EXECUTIVE PRODUCER ..... Shyama Helin

CREATIVE DIRECTOR ..... Sandy Winkelman

WRITER ..... Brian David Johnson

PRODUCTION COORDINATOR ..... Steve Buccellato

SPECIAL ADVISOR ..... MAJ Jessica I. Dawson, Ph.D.

ARTISTS ..... Rafael Pimentel
Vicente Cifuentes Martinez
Giuseppe Cafaro

COLORIST ..... Rex Lokus

ACKNOWLEDGMENTS

Thank you to all the experts and contributors who provided the team with invaluable ideas, insights, and technical knowledge.

MAJ Jessica I. Dawson, Ph.D.
COL Natalie Vanatta, Ph.D.
LT COL Jason Brown, Ph.D.
Jamie Carrott
Cory Doctorow

Phaedrus LLC:
John Marx
Alex B. Ruiz, CISSP, GCIH
Todd Stratton

Arizona State University:
The School for the Future of Innovation in Society
The Center for Science and the Imagination
The Applied Research Lab (ASURE)
The Threatcasting Lab

Army Cyber Institute at West Point, 2023

First Edition, 2023

https://cyber.army.mil

Army Cyber Institute at West Point
www.cyber.army.mil

Threatcasting Lab
at Arizona State University
www.threatcasting.com

Arizona State University
www.asu.edu

Phaedrus
www.phaedrusllc.com


THE ARMY CYBER INSTITUTE AT WEST POINT
2012
ARMY CYBER
INSTITUTE
AT WEST POINT