THE CIPHER BRIEF

Fourth Generation Espionage: The Making of a Perfect Storm

Val LeTellier / Aug 3, 2021

In a rare December 2018 public address, British Secret Intelligence Service (SIS) Chief Alex Younger used the term 'fourth-generation espionage' to describe the new mindset that intelligence leaders needed to address the challenges of the fourth industrial revolution.

He noted that "The digital era has profoundly changed our operating environment. Bulk data combined with modern analytics make the modern world transparent. We need to ensure that technology is on our side, not that of our opponents". [1]

NEW TECHNOLOGIES = CHANGING ESPIONAGE TACTICS

Younger's concerns are well founded. The Fourth Industrial Revolution includes many new technologies that complicate clandestine activity, including "mobile devices, Internet of things (IoT) platforms, location detection technologies (electronic identification), advanced human-machine interfaces, authentication and fraud detection, smart sensors, big analytics and advanced processes, multilevel customer interaction and customer profiling, augmented reality/ wearables, on-demand availability of computer system resources, and data visualization." [2]

In fact, the combination of ubiquitous digital surveillance and powerful data analytics is changing espionage in ways that we are only starting to understand. What we do know is that widespread automated recognition and monitoring of individuals is now possible, 'blind spots' are quickly being eliminated, events can be forensically examined to the degree never known, and an individual's future actions quickly and accurately predicted.

This comes through expansive closed-circuit television (CCTV) camera placement, 'smart city' technologies, ad-tech data, vehicular telemetry, IoT, and 5G networks enabling omnipresent personal data collection and the data analytics to make sense of it all; machine learning that enables massive data aggregation, facial recognition for real-time monitoring and post-event investigation and pattern analysis for identifying anomalies and predicating behavior.

Finally, the artificial intelligence (AI) capabilities, 'multi-intelligence fusion' methodologies and correlation engines currently under development will certainly enable counterintelligence by further empowering aggregation and seamlessly integrating different sensor types.

DIGITAL STORM CLOUDS BUILDING

Law enforcement and counterintelligence elements now have an exponentially growing array of digital sensors and robust analytics to collect and turn massive data pools into usable information, allowing them to increase accountability within their governments, prevent external and internal actors' activity, and quickly investigate suspect activity.

This 'perfect storm' of exploding data collection, powerful data analytics and even virus tracking creates what some have called 'an existential threat' to the ability of intelligence agencies to conduct mission. To better understand these challenges and what intelligence agencies need to do to address them, it is helpful to examine the impact of the new operating environment on select human intelligence activities:

First, think about widespread personal data collection and the impossibility of privacy and effective cover. Advanced data analytics, machine learning (ML) and AI enable the aggregation of massive data sets, the correlation of activity and the real time and forensic exposure of operations. High-speed/high-density 5G cell networks, IoT devices and vehicle telemetry provide refined triangulation and location of an individual's movement, further complicated by emerging issues like DNA mapping and virus tracking.

Second, think about the massive expansion of the virtual domain where many people now spend more time than the physical world. The ability to operate safely, securely, sustainably, and successfully online are 'table stakes' for any modern-day service, underpinning a wide spectrum of activity like information collection, targeting, influencing, and recruiting. COVID's restrictions have only accelerated and reinforced this point.

Meawhile, cyberspace is becoming more active, unforgiving, and hostile. Data providers and social media platforms are monetizing their access through stronger authentication and adversary services are increasingly aware of traditional methodologies. Emerging national Internet networks in Russia and China challenge the ability of intelligence agencies to electronically travel there. Generative adversarial networks (GANs) are enabling advanced deepfakes and impairing the ability to detect false information/personas and tailored social engineering.

Finally, blockchain and cryptocurrency enable non-attributed payments and complicate the ability to "follow the money" and quantum computing can threaten communication security tools and enable the decryption of what was one secure data collected by adversaries.

Now think of these not as single problems you have the luxury of time to address one at a time, but as concurrent challenges simultaneously undermining traditional tradecraft methodologies. The challenge is daunting.

Bottom line, these challenges require a new approach and innovation. The speed of change in this domain is remarkable, meaning that operators constantly need increasingly sophisticated support for an increasing breadth and depth of challenges.

NEW OPERATING ENVIRONMENT REQUIRES INTELLIGENCE TO EVOLVE

Specifically, different solutions are needed for different missions to identify, quantify, and mitigate digital surveillance risk ranging from growing big data aggregation to street level 'smart city' applications.

For virtual operations, intelligence agencies need to counter ever-changing and evolving authentication measures by social media platforms, including biometrics and liveliness tests. These changes

further test their ability to look real to platforms, targets, and adversaries and achieve scalability, and practice an 'art form' that requires a choreographed blend of technology, talent, and tradecraft.

That said, the news isn't all bad. Some elements of this new tradecraft should come naturally as intelligence agencies leverage 'technological reciprocity'; offensive solutions enabling defensive solutions and vice versa. For example, by developing refined digital targeting one can inform the development of digital surveillance countermeasures, by developing specialized payment mechanisms one can strengthen one's understanding of adversary payment tradecraft, by applying new data analytics one can reveal adversarial data methodologies and vulnerabilities, and by red teaming one's processes one can reveal indicators for adversary activity identification.

Traditional tradecraft is already being publicly proven inadequate for today's new operating environment, reinforcing that the arrival of the fourth industrial revolution is an inflection point for intelligence services; separating those that harness advancing technology to their advantage from those that fall victim to it. American intelligence services must also "evolve or die" to maintain the degree of effectiveness and relevance they've had up to the present.

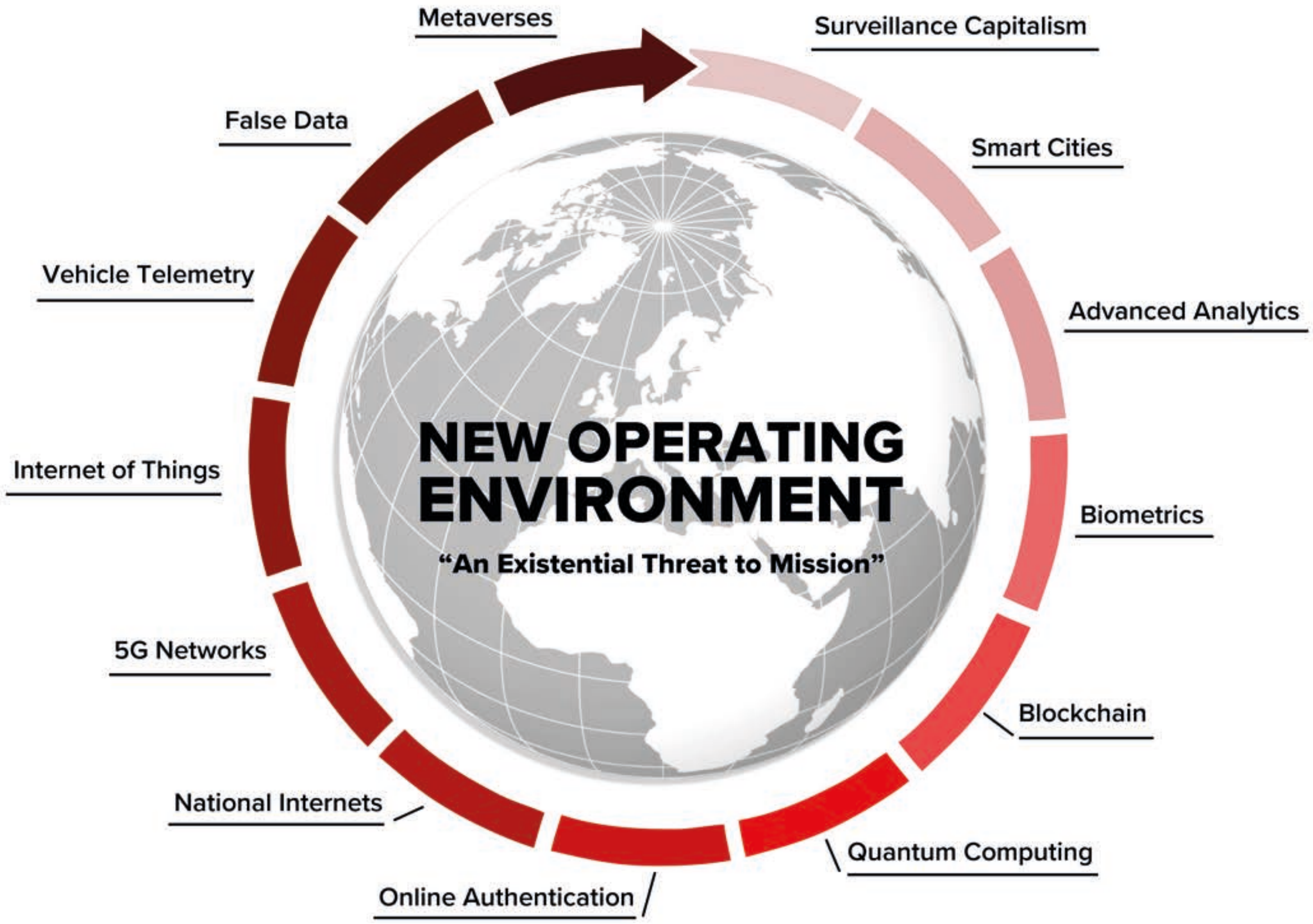
First, they must make their workforces aware of the impact of the modern technologies upon their respective missions and then invest the necessary resources to develop 'next generation tradecraft' methodologies, capabilities and solutions to counter or harness specific technologies against operational goals.

Given that the technological advancement we're witnessing is predicted to only accelerate under its own momentum into the coming decades, falling behind on these responses will have long lasting impact to each organization's capacity to execute mission and the overall strength of the United States Intelligence Community.

[1] Alex Younger, 3 December 2018 https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage.
[2] Wikipedia, June 2021

Val LeTellier is a veteran intelligence officer. Before his career as a CIA case officer, he served as a State Department Diplomatic Security Special Agent. He has since worked with CACI, Booz Allen and Raytheon in creating specialized communication, virtual operations, and digital surveillance risk mitigation programs. His current focus is developing next generation tradecraft capabilities for IC front-line operators.

Now think of these as concurrent challenges --
not single problems you have the luxury to address one at a time.



- ***Surveillance capitalism.*** *Think the impossibility of cover. Think real time/ forensic exposure of operations.*
- ***Smart City Applications.*** *Think about finding the needle in the haystack, and in a second.*
- ***Facial/Gait Recognition.*** *Think instantaneous recognition.*
- ***DNA Matching.*** *Think definitive identity correlation.*
- ***Quantum computing.*** *Think breakdown of communication security and decryption of past data.*
- ***Blockchain/cryptocurrency.*** *Think non-attributed payments and an inability to "follow the money".*

- ***Advanced analytics, ML/AI.*** *Think aggregation of massive data sets, fusion of unstructured data and correlation of travel and activity.*
- ***Social media authentication:*** *Think SMS text from a SCIF was hard? Try video and biometrics.*
- ***Emerging national Internets.*** *Think Russia, China and the inability to virtually travel there.*
- ***GANs.*** *Think advanced deepfakes and the inability to detect false information/personas and tailored social engineering.*
- ***Fast and dense 5G networks.*** *Think refined triangulation and location of your movement.*

NEEDED: NEXT GENERATION TRADECRAFT SOLUTIONS

UBIQUITOUS TECHNICAL SURVEILLANCE

Omnipresent CCTV cameras, 'smart city' technologies, ad-tech data, vehicular telemetry, IoT, and 5G networks enable ubiquitous personal data collection and surveillance. Facial/gait recognition, biometrics, advanced analytics and multi-intelligence fusion make sense of it all. The result is massive data aggregation and pattern analysis for real-time monitoring, post-event investigation, anomaly identification and behavior prediction. Together, this creates 'an existential threat' to mission success. These are not 'one size fits all' problems.
Different missions require different solutions to identify/quantify/mitigate surveillance risk in real-time.

CRYPTOCURRENCY/BLOCKCHAIN

Cryptocurrency challenges traditional 'follow the money' methodologies, while affording anonymity to IC transactions. The great potential value of the blockchain to intelligence is only now being recognized and explored.
Defensive and offensive capabilities are needed; payment tracking and truly anonymized payments.

VIRTUAL OPERATIONS

The ability to operate safely, securely, sustainably and successfully online is a core competency for intelligence organizations, underpinning a wide scope of activity that includes data collection, target engagement and influencing. Platform authentication, target and adversary awareness, reverse image forensics, deepfakes, and data poisoning significantly challenge mission execution.
Platforms must seamlessly fuse the unique technology, talent and tradecraft required for the 'art form' that is modern online operations.

SPECIALIZED DATA COLLECTION AND ANALYSIS

Despite the IC's availability of massive data streams and lakes, a shortage exists for timely provision of unique and enriched data sets and more refined products. Analytical elements must be enabled to efficiently and effectively conduct Bellingcat-type investigations.
Holistic data solutions must incorporate advanced data analytics earlier in the delivery chain.

INSIDER RISK

Continuous evaluation fueled by advanced analytics is the future of insider risk mitigation. The fusion of internal and external data provides insights into predispositions, associations, intentions, plans and actions, and early warning of cases that require attention before they become a threat to information, assets, people, facilities or themselves.
Holistic insider risk solutions must fuse internal indicators, public data and advanced analytics.

THE UTS MITIGATION DOMAIN

CRITICALITY TO 'FOURTH GENERATION ESPIONAGE'

Digital surveillance and powerful data analytics enable real-time identification and monitoring of individuals.

Events can be forensically examined, and an individual's future actions quickly and accurately predicted.

Expanding Smart City apps, 5G networks, biometric sensors, and enhanced facial recognition drive continued threats.

Literal and virtual 'blind spots' are quickly being eliminated.

KEY CHALLENGES

To operate clandestinely in the New Operating Environment, real-time identification, quantification and qualification of digital surveillance risk is critical for operational planning and forensic analysis.

CRITICAL MISSION COMPONENTS

ADVERSARY CAPABILITIES

Offensive/defensive , Public/proprietary data, Hacked accesses

USER INTERFACE

Single-pane surveillance risk dashboard display.
Digital surveillance risk overlaid on city maps, ranked by color.
Icons provide details on specific threats.

OPEN-SOURCE DATA PUBLIC UTS CAPABILITIES

Smart City Apps, Public Transportation, License plate readers
Ad-Tech, CCTV, etc.

PROPRIETARY DATA NON-PUBLIC UTS CAPABILITIES

Travel and immigration records, Financial transaction records, Hacked/leaked data, Cell network data, Vehicle telemetry, etc.

THE BLOCKCHAIN DOMAIN

CRITICALITY TO 'FOURTH GENERATION ESPIONAGE'

Tracking cryptocurrency is critical to modern 'follow the money' investigations. Truly anonymous payments remain critical to successful source and procurement operations. The significant value of the Blockchain methodology to HUMINT is yet unrealized.

KEY CHALLENGES

The Blockchain and cryptocurrency is designed for anonymity. Effective analysis requires rapid aggregation and correlation of multiple data sets. To be scalable, analysis requires robust analytics and automation. The importance and applicability of Blockchain and cryptocurrency is not well understood.

CRITICAL MISSION COMPONENTS

Data correlation
Thousands of money movements and wallet transactions, volumes of proprietary data and PAI collected and correlated for connections.

Data
Proprietary, Public

Analytics
Algorithms, Machine learning, Artificial Intelligence

SMEs
Cryptocurrency, Blockchain, Technical

Operational reciprocity
Leveraging innovative tracking capabilities to make truly anonymized payments.

Relevancy
Ensuring that analytical methodologies and software are cutting edge.

Blockchain for HUMINT
Data is preserved in an unalterable and decentralized form secure from supply chain events, a uniquely valuable tool for HUMINT processes.

THE VIRTUAL OPERATIONS DOMAIN

CRITICALITY TO ‘FOURTH GENERATION ESPIONAGE’

The ability to operate online in a safe, secure, successful and sustained manner is critical to recruitment, influencing, and open-source collection operations.

KEY CHALLENGES

- Looking real to platforms, targets and adversaries.
- Staying ahead of advancing/evolving authentication measures.
- Scaling with differentiated signatures/solutions
- Mastering an ‘art form’ that fuses technology, talent and tradecraft.

CRITICAL MISSION COMPONENTS

Personas

Realistic, deep and mature, robust unique content.

Multifaceted and flexible backgrounds.

Synchronized content, subscriber data, points of presence.

Foreign social media platforms.

Talent

Social media, Operational, Technical

Tradecraft

Technical Engagement, Vetting, Governance, Training

Infrastructure

Specialized procurement

Managed attribution network

Global hubs and edge nodes

Foreign mobile numbers

Synchronized metadata

Operator workstations

Authentication

Avoidance/countering of SMS and CAPTCHA challenges.

Prep for selfie, liveliness, voice, and biometric challenges.

Early warning of new authentication procedures.

Early warning of emerging concepts.

Early warning of new authentication procedures.

Early warning of emerging concepts.

Red Teaming

Personas, Infrastructure, People, Processes

Facilities

Commercial, Dark fiber, SCIF

THE SPECIALIZED DATA DOMAIN

CRITICALITY TO ‘FOURTH GENERATION ESPIONAGE’

The ability to operate online in a safe, secure, successful and sustained manner is critical to recruitment, influencing, and open-source collection operations.

KEY CHALLENGES

- Discovery of uniquely valuable data.
- Clear and concise data presentation.
- Scalability to meet exponential global data growth.
- Aggregation of unstructured foreign language data.
- Growing authentication procedures and national Internets.

CRITICAL MISSION COMPONENTS

Presentation

Low to High Side Transfer
User Interface

Tradecraft

Governance, Red teaming,
Training

Infrastructure

Automated collection

Automated aggregation

Obfuscated retrievals

Foreign language translation

Global proxy network

Bots

Detection mitigation

SMEs

Data science, Intel analysts,
Social media, Technical

Analytics

Algorithms

Fusion technology

Machine learning

Artificial Intelligence

THE CONTINUOUS EVALUATION DOMAIN

CRITICALITY TO ‘FOURTH GENERATION ESPIONAGE’

Continuous Evaluation (CE) offers a dynamic, real-time, early warning of potential insider risk, replacing the single periodic investigations ‘snapshots’ taken every five-seven years. In a growing remote work environment, behavior changes are increasingly less visible to colleagues and managers.

KEY CHALLENGES

The body of relevant public data is constantly evolving.
Public data collection must be properly messaged to the workforce.

CRITICAL MISSION COMPONENTS

Presentation

Low to High Side Transfer
User Interface

Tradecraft

Governance, Red teaming,
Training

Infrastructure

Automated collection

Automated aggregation

Obfuscated retrievals

Foreign language translation

SMEs

Data science, Intel analysts,
Social media, Technical

Analytics

Algorithms

Fusion technology

Machine learning

Artificial Intelligence