

## **One Operator Cannot Resist the Surveillance Economy: UTS and the Human Domain in Irregular Warfare**

**Abstract:** Irregular warfare doctrine has long affirmed the primacy of the human operator over technological systems. Yet the surveillance economy - characterized by ubiquitous technical surveillance (UTS) across visual-physical, electronic, financial, travel, and online domains - constitutes a comprehensive personal threat that doctrine has not fully addressed. This paper argues that the five primary vectors of UTS possess direct personal corollaries in the physical, psychological, emotional, relational, and digital domains of the individual operator, and that failure to account for these personal dimensions produces operators who are technically proficient but operationally deficient in the judgment irregular warfare requires. Human primacy demands institutional grounding in human-centric doctrines - signature reduction and digital force protection - capable of matching the scale of the environment operators cannot individually resist.

### **The Surveillance Economy Versus the Operator**

Irregular warfare necessitates sound operator judgment under ambiguous and uncertain conditions. It often expects, even demands, disproportionate effects from small teams operating under little-to-no guidance. But singleton operators and small teams cannot effectively resist an economy. Yet, that is the promise when operators and small teams are outfitted with the latest technology designed to help them keep pace with the demands of modern warfare. The environment which characterizes modern warfare is that of [ubiquitous technical surveillance](#) (UTS). The challenge for operators and teams, then, is to employ technology within the surveillance economy while maintaining freedom for action. Operators must understand the effects of UTS universally and personally. Those who are not grounded in an adequate human-centric doctrine risk becoming something other than what irregular warfare requires. They will be technically proficient but deficient in operational judgment, and thus, maneuver.

Our aim here is to examine the personal effects of UTS on the operator so as to understand how to maintain his freedom. We do this by interpreting the five UTS vectors in light of the individual operator. This is ultimately grounded in the doctrine of signature reduction and its operationalized form of digital force protection. [Signature reduction](#) is the management of digital and physical signatures across domains to enable operational maneuver under conditions of UTS. [Digital force protection](#) (DFP) is its operational form, the practical human discipline which minimizes the attributable surfaces exposed by UTS and preserves operational maneuver across the full spectrum of operations. Signature reduction and DFP are the lens through which we understand technology, human primacy in irregular warfare, and the dynamics of their interaction.

### **The Human Domain: Five Personal Corollaries**

Within the surveillance economy we speak of five primary cross-domain vectors by which operators are collected against, correlated, and attributed to determine their identity, location, network, and ultimately, intent. This process, both the [attribution chain](#) by which operators are deformed, and the broader environment within which operators fight, we call ubiquitous technical surveillance. The five primary UTS vectors traditionally examine the technical risk exposure of an operator or organization's signature across visual-physical, electronic, financial, travel, and online domains. Each one presents an attack surface an adversary can exploit. Different terminology may be substituted for each of these domains, but the emphasis remains: UTS is cross-domain, persistent, and tough to beat. It appears not only to characterize the environment but constantly pressures whosoever operates in our contemporary post-digital age.

This pressure has its cost: each of the five UTS vectors characterizes an aspect of the surveillance economy—the sum total of surveillance ecosystems, processes, technologies, and actors who function within it for profit or other ulterior motives—that corresponds to a culminating effect in the human domain. Indeed, because he operates within the surveillance economy and seeks greater freedom for action within it, the contemporary operator experiences a personal degradation of his operational capacities. It strikes him from within and without. This is evident not only in the study of our discipline of [signature reduction](#) and UTS, but also across broader irregular warfare disciplines. The burgeoning public awareness of [cognitive warfare](#) is one such example, an aspect of unrestricted warfare in which the decisive battleground is human perception and understanding itself. Amidst a complex digital domain, narrative power is used as currency and pretext for action in the physical. Adversaries use technology to shape others’ understanding, according to their desired outcomes.

For his part, the operator expects a fight. He willingly withstands and even expects such conditions, and fights as long as he is able using the resources, training, and skills at his disposal. Nevertheless, that which may have once been a condition is now environmental. In a conflict where the [battlefield is everywhere](#), the operator simply cannot sustain his effort—one person cannot scale in proportion to the environment in which he operates. UTS makes this clear: adversaries have systematized and institutionalized the operational environment as one defined by the surveillance economy. One person cannot resist an economy. The five UTS vectors thus possess personal implications for the operator which synthesize across the human domain.

We only introduce and characterize five personal domains here for further development: the physical, psychological, emotional, relational, and digital. Each of these mirror the adversarial conditions and cross-domain vectors of UTS but at personal scale. What remains is to grasp the damaging effects on the individual operator in this environment so as to set the conditions to train and equip him, by way of digital force protection and signature reduction, to maneuver with greater freedom for action within the surveillance economy.

### ***Physical: Threat to Maneuver***

The visual-physical vector of UTS applies here but personally. The operator recognizes the environmental threats to his freedom of maneuver, especially abroad or in contested operating areas, and as a result, curtails his movements. Acknowledging the ubiquity of visual-physical technologies which capture his movements, dress, gait, face, and person not only abroad but also at home, physical movements—even non-operational ones—require greater risk management. Organizations of which he is a part also grasp this potential threat, and impose policy-based restrictions derived from overly risk oriented decision-making. This ultimately serves to increase the cost the operator and his team must spend to mount an operation, and mission effectiveness falls as a result. Digital force protection acknowledges these threats to freedom of maneuver and accepts them, while strengthening and conditioning operators in both awareness and practical skills they can employ to mitigate these threats. Increasingly complex operating environments do not negate the necessity of fundamentals. This manifests through daily practices such as operator mindfulness of routines and patterns of life both physically and digitally; and when appropriate, employing force protection routes to manage one’s physical signature in accordance with desired maneuver objectives.

### ***Psychological: The Battle Within***

The psychological aspect correlates with the electronic vector of UTS. The example which mirrors the phenomenon is the cognitive warfare mentioned above. As a result of constant exposure to an unregulated information environment mediated by electronic technology, the psychological domain sees the operator forced into competition within himself. Specifically, the battle is his internal

understanding of the environment and its effects on his operational capacities. Conditions of UTS now possess a personal mode forced on him via the technology he uses. At its worst, the operator now experiences and internalizes the uncertainty, doubt, and operational confusion of the environment. This paralyzes his operational initiative and damages mission effectiveness. Digital force protection does not minimize the personal psychological effects of attribution pressure, but places signature management back in the hands of the operator as a means to resist it. He does not require unlimited access to data, or more information to make operational decisions, and finds he can intentionally limit device employment in personal and operational contexts to strengthen his operational decision-making and orientation to the environment.

### ***Emotional: Willingness to Fight***

This is the personal mode of the financial UTS vector. The emotional composition and disposition of an operator ultimately inform his willingness to fight and bear ambiguity and uncertainty. They inform his demeanor, attitude, and govern to some extent his operational behavior in an adversarial environment, or his willingness and desire to train for it. The operator's emotional content is the internal, integral, inter-relational, and truly personal currency which he exchanges for motivation and willingness to fight amidst adversarial conditions. However, if these conditions become prolonged, systemic, and environmental, the operator can be led to a disposition of weakened resolve and morale. When every personal "transaction" is monitored or could be inferred from technology that is external to him, the operator surrenders hope for mission success and is defeated before operations begin. Digital force protection accounts for each personal technological interaction and promotes management of the operator's holistic signature: it serves to safeguard his maneuverability in digital terrain. So long as the operator possesses maneuver, he is free to act towards operational ends.

### ***Relational: The Erosion of Alliances***

This aspect is represented by the travel vector of UTS. An operator's true power is the relationships he builds and maintains so as to remain close to the ground truth, and in the alliances he forms which allow him to conduct coordinated and complex operational maneuvers. Taken more practically, in previous times it was possible to travel and preserve relative discretion and privacy in pursuit of operational objectives. Under invasive technological conditions, however, this is increasingly prohibitive. Every interpersonal interaction or alliance is no longer known but scrutinized and called into question. Operators no longer possess the relative freedom of maneuver to form coalitions, liaise with foreign counterparts, or engage as fully with partner forces with sufficient discretion necessary to build durable new alliances. Digital force protection sets the conditions within which alliances can be formed and safeguarded with appropriate measures.

### ***Digital: Ubiquitous Risk Without Boundaries***

The final personal domain mirrors the online vector of UTS. An operator's exposure to the digital domain is the extent to which he is exposed to potential risk. So long as he employs digital technology does he and his mission remain potentially at-risk. The online vector and the digital domain it leads to is a vehicle, and how the operator drives it informs the extent to which this potential risk becomes actualized in operational contexts. Yet, due to the ubiquity of digital technology, this risk potential extends not only in traditionally contested environments but across the entire surveillance economy. The operator is at-risk at home and abroad—whenever he uses digital technology regardless of the end. Digital force protection promotes a holistic discipline for technology use which not only considers and thrives in operational contexts but which actually begins in personal ones. It does not

significantly change nor require extensive resourcing employed abroad or at home-station. Rather, it understands the ubiquity of attribution pressure and offers counteroffensive maneuverability which begins at home and extends abroad.

### **From Operational Problem to Institutional Doctrine**

The decisive terrain of human judgment is not the sole responsibility of the operator, though he is in many ways closest to the problem. It also requires institutional backing which sets the conditions for operator judgment to grow. For this reason the doctrine of signature reduction must have a home in its operational and institutional manifestation, the discipline of [digital force protection](#). Without operational and doctrinal grounding in human-centric doctrines such as [signature reduction](#) and digital force protection, technology use will prove more distracting than contributive to operational objectives. In the long-term, it will prove damaging to operational judgment and decision-making from the individual to organizational levels.