SAMPLE

Building the Cyber Warfare of Tomorrow

The War Beneath the Signal

Aiman JoeHanz

Free sample: Introduction & Chapter 1

putrabooks.github.io

Buy the full book:

Carousell carousell.sg/p/building-the-cyber-warfare-of-tomorrow-ebook-pdf-1471335774

Ko-fi

Payhip

Contents

Introduction

Chapter 1: The Definition and Its Impostors

Chapter 2: The Terrain

Chapter 3: The Arsenal

Chapter 4: The Kill Chain

Chapter 5: The Defense in Depth

Chapter 6: The Attribution Problem

Chapter 7: The Doctrine

Chapter 8: The Economics

Chapter 9: The Critical Infrastructure

Chapter 10: The Decade Ahead

Introduction

Every previous volume in this series has described a machine built to be used. This one describes a machine built to be used and attacked - because the same wires that carry the civilization's work also carry its wars, and the network that eliminated distance for commerce eliminated it for conflict as well. Cyber warfare is the newest form of the oldest human practice, conducted on a terrain that runs beneath every other technology this series has covered: the smart home is attacked through its hub, the robot through its controller, the telecommunications network through its switches, the semiconductor plant through its design files, and the software through its own supply chain. The reader who understands the anatomy of conflict in the networked age therefore understands the vulnerability of every other anatomy in the catalog.

The subject is unusually rich in impostors, so the definition deserves its own chapter before anything else. Most of what the news calls cyber warfare is not warfare: it is crime seeking profit, espionage seeking information, or vandalism seeking attention, and the distinction is not pedantry - each impostor behaves differently, responds to different pressures, and demands a different defense. Warfare proper - organized force applied for political ends - occupies a narrow band of the spectrum, and the book's first instrument is the ability to tell the band from its neighbors. The second instrument is the terrain habit: the attacker does not live in a legal abstraction but on specific machines, in specific credentials, along specific supply chains, and every argument about cyber conflict becomes concrete when placed on the terrain it is actually about. The third instrument is the economics habit: the attacker's work is priced like any other industrial process - reconnaissance, tooling, labor, delivery, cleanup - and the defense that raises the attacker's price survives, while the defense that only raises the defender's own cost does not. These three instruments - the definitional, the topographic, and the economic - are the lenses the book carries through every chapter.

The ten chapters build in the order a practitioner meets the subject. The first chapter sets the strict definition and separates it from its impostors. The second walks the terrain: the attack surface as a geography, the layers of it from the endpoint to the supply chain, and the properties that make networked terrain unlike any terrain armies have met before. The third catalogs the arsenal: the taxonomy of weapons, what each is physically, and what each is for. The fourth follows the intrusion itself from reconnaissance to objective - the kill chain, the phases every real intrusion passes through, and

the places each phase can be broken. The fifth builds the defense in depth: the layered doctrine, the maintenance that is the defense's real face, and the honest limits of what patching and hygiene can and cannot do. The sixth takes up the hardest problem in the field - attribution - and shows why it is an intelligence discipline rather than a laboratory result, and how deception lives inside every answer. The seventh turns to doctrine: deterrence and its failure modes, escalation and thresholds, and the legal categories states actually argue in. The eighth prices the whole conflict: the asymmetries of cost, the markets that trade in vulnerability, and the insurance logic that is quietly reshaping the defense. The ninth walks the critical infrastructure - the grids, the water, the transport, the hospitals - where the network's failures become the physical world's failures, and where the next decade's real stakes live. The tenth closes with the decade ahead: the machinery that will matter, the honest uncertainties, and the operating program a builder, defender, or official can run when the noise arrives.

The series makes three promises everywhere in its catalog, and this volume keeps all three. No vendor names: the book names no product, no company, no incident by its brand, because the structure of an intrusion does not depend on which vendor's logo sat on the machine, and the reader who learns structure can apply it to any vendor's machine. No expiring statistics: every number in the book is either a structural constant - a property of the physics or the economics - or is explicitly labeled as an illustrative scale of magnitude, so the text does not rot. No forecasts dressed as facts: the decade chapter offers structure and labeled uncertainty, because the reader who reaches this book's last page should be able to take any headline to pieces down to its structural facts within a few sentences, and that ability - the series calls it structural literacy - is the only durable defense against a subject whose headlines change weekly while its structure has barely moved in a generation.

Read the chapters in their printed order, since each one spends a trust the one before it earned: the doctrine chapter's thresholds only make sense after the attribution chapter's uncertainties, and the economics chapter's asymmetries only make sense after the arsenal and kill chain chapters' mechanics. A reader holding a particular decision may enter directly: the executive weighing a security program should read the defense and economics chapters first; the engineer building defenses should read the terrain, arsenal, and kill chain chapters together; the official or student thinking about policy should read the definition, attribution, and doctrine chapters as one unit. Each chapter ends with one closing page that distills its argument to a size the reader can keep,

and the reader holding only those ten distillations at the end holds the book's working core.

Chapter 1: The Definition and Its Impostors

Warfare conducted through information systems is best defined by its ends, not its means. The strict definition this book uses: cyber warfare is organized hostile action, taken through or against information systems, intended to coerce a political community or degrade its capacity to act, under the authority of a political actor. Every clause of that definition does work, and the chapter builds the definition clause by clause, because the impostors fail it at specific, knowable points.

Organized means the action is resourced, staffed, and directed - a program, not a mood. Hostile action means the intent is to harm: to damage, disrupt, deny, degrade, or destroy. Through or against information systems covers both the intrusion that travels the network and the physical attack on the machines themselves, because a war on the network includes the wires as much as the packets. Intended to coerce a political community is the war aim: the actor wants the community to do something it would not otherwise do, or to lose the capacity to do something it wants to do. Under the authority of a political actor separates the state - or the proxy the state arms, or the movement the state shelters - from everyone else who happens to hold the same tools.

With that definition in hand, the impostors sort themselves in order of closeness. Cybercrime is the nearest impostor because its tradecraft is identical: the same intrusion chain, the same implants, the same persistence. What differs is the aim - profit rather than coercion - and the difference matters operationally, because the profit motive gives the criminal a horizon the warrior lacks: the criminal must monetize, and monetization creates customer service, negotiation, payment infrastructure, and other surface the defender and the police can work. The warrior has no monetization to interdict; the intrusion that will be used for sabotage looks exactly like the intrusion that will be used for theft, right up to the instant it suddenly is not. The honest consequence: at the moment of intrusion, the defender often cannot know which impostor is inside, and must defend as if the worst case were true - the first of many places where the definition problem is really a defense problem.

Cyber espionage is the second impostor, and the hardest to separate, because espionage and war are both political acts under state authority. The traditional line is acquisition versus alteration: espionage takes copies and leaves the world as it found it, while warfare changes the world - breaks the machine,

corrupts the data, drops the grid. The line is honest but thinner than it looks. Intelligence stolen can be weaponized elsewhere; a design file copied is a factory built by someone else; and the reconnaissance that maps a power grid for intelligence today is the targeting data for the sabotage of tomorrow. The reader should hold the line and its thinness together: espionage is not war, but the same access supports both, which is why states treat the espionage-layer intrusion into critical infrastructure as a war-level concern even when nothing has yet been altered. The third impostor is hacktivism and vandalism - attention-seeking and anger-seeking, organized loosely or not at all, aiming at neither profit nor political coercion in the strict sense - and the fourth is the insider, who needs no intrusion at all. Each fails the definition at a different clause, and the defender who cannot sort them will misprice all four.

One more term needs its place before the terrain chapter: the gray zone, the band between espionage and war where most state conduct actually lives. Below the war threshold sits a continuous spectrum of hostile action - harassment, doxxing, disruption of services, spoofing of information, small sabotage timed to stay under headlines - and states spend most of their networked effort there, precisely because the actions are individually deniable and collectively coercive. The gray zone is not a failure of the definition; it is what the definition predicts: coercion is cheapest below the threshold at which the target feels entitled to shoot back. The book returns to this logic in the doctrine chapter, but the reader should carry the shape of the spectrum from here forward: crime at the bottom, espionage and gray-zone coercion in the middle, sabotage rising, war at the top - and the same tradecraft serving every band.

Why the Definition Fights Its Impostors

The definitional discipline earns its keep at the moment of response, and the chapter should show the fight explicitly rather than assert it. When a hospital's scheduling system fails, the first question is not who but what kind: a criminal encrypting for payment, a vandal defacing for attention, or a warrior preparing the ground for something larger. The three impostors summon different reflexes. The criminal wants the hospital's payment and will, within its own distorted customer-service logic, help restore the records once paid - the intrusion is a negotiation wearing a weapon's clothes. The vandal wants the spectacle and will announce it. The warrior wants the disruption itself and may have built the failure so that restoration is beside the point - no payment is coming, and the effect was scheduled to arrive at the worst hour. An

institution that responds to the warrior with the criminal's playbook - pay, wait, restore - loses days it does not have, and an institution that responds to the criminal with the warrior's playbook - hunt, escalate, treat as war - spends scarce focus on an actor whose whole business model is to be found and paid. The sorting, in other words, is not academic hygiene; it is the triage that decides the first forty-eight hours.

The public vocabulary works against this triage, and the reader should understand why. Attack attaches to any intrusion the prefix cyber and any intrusion the word war, because both inflate: the prefix borrows the story's technical authority, and the word borrows its gravity. A generation of headlines has therefore flattened a spectrum into a single alarm, and the flattening has policy consequences - budgets built for war get spent on crime, and instruments built for crime get aimed at war - and the reader who can hold the spectrum against the headline's flattening is already ahead of most of the commentary. The series' habit applies: read the claim for its structure, not its vocabulary, and ask which actor, which aim, which threshold, before accepting the label.

The state's vocabulary deserves the same audit, because states have their own reasons to blur. An actor conducting espionage prefers the cover of crime - burglars are pursued by police, spies by governments, and the police option is cheaper to be caught by. An actor conducting gray-zone coercion prefers the cover of nature - the outage, the accident, the crowd of anonymous patriots - because deniability is the coercion's discount. And an actor caught preparing for war prefers the cover of research, security testing, or network hygiene, which is the gray zone's oldest suit. The definition chapter's sorting instrument therefore reads state claims with the same skepticism it reads headlines: the label a state applies to its own conduct is a policy choice, and the structural reader asks what the conduct does, not what the ministry calls it.

The Reader's Three Instruments

Because the definition is a lens rather than a verdict, the chapter should equip the reader with the three questions that operationalize it, and these three questions recur in every later chapter. First, the aim question: what does the actor want - payment, information, attention, or coercion? The aim is visible in the intrusion's behavior long before any actor is identified: the exfiltration profile says information, the encryption-plus-contact says payment, the defacement-plus-announcement says attention, and the quiet positioning

inside a control network says coercion. Second, the authority question: who can order this - a state, a proxy the state can restrain, a market the state tolerates, or a person the state has never heard of? The answer determines which instruments apply - diplomacy, law enforcement, sanctions, or nothing yet - and it is the question most often skipped in public argument. Third, the threshold question: has the conduct crossed into the domain where force is a legitimate answer? The threshold is set by the target's doctrine and the attacker's knowledge of it, which makes it partially subjective, and honest analysis says so rather than pretending a bright line exists. The book's later chapters build each instrument: the terrain and kill chain chapters sharpen the aim question, the attribution chapter sharpens the authority question, and the doctrine chapter sharpens the threshold question. Together they are the definition working - a sorting discipline a reader can carry into any incident the decade produces.

A Structural Reading of the Public Record

The public record, read structurally rather than by name, gives the definition its evidence, and the reader benefits from seeing how the sorting works on episodes everyone half-remembers. An air-gapped enrichment facility whose centrifuges were destroyed by code is the record's clearest war-use of the networked instrument: physical destruction, political aim, state program - the definition met in full, whatever the diplomatic silence around it. A national grid darkened twice in the same country within a decade, once on the record as a deliberate attack, once ambiguous, is the record's lesson in thresholds: the same target, the same techniques, and the difference between war-support and gray-zone coercion was less in the code than in the politics around it. A global ransomware epidemic that shut hospitals, shipping, and factories without any war aim at all is the record's reminder that the impostor can out-damage the warrior: the criminal's indifferent blast radius exceeded every state sabotage in the same period, and the hospitals were collateral that no coercion intended. And a decade of industrial espionage that stripped one economy's designs into another's factories is the record's demonstration that the espionage impostor, multiplied across thousands of intrusions, can shift more wealth than any sabotage campaign - while remaining, in strict doctrine, not war at all.

The episodes sort cleanly by the definition, and the sorting is the education. The reader notices first that the record's biggest effects came from the impostors, not the warriors - a structural fact the decade's threat inflation

never mentions. Second, that the warrior's work is patient and rare: the destruction of centrifuges was preceded by years of quiet positioning, and the grid attacks by years of reconnaissance - warfare in the networked spectrum is mostly preparation that becomes an event rarely, which is why the peacetime defense posture matters so much, since the preparation happens against you in peacetime. Third, that the boundary moves: the espionage that copies a design and the sabotage that breaks a machine used the same accesses, and the record shows states converting espionage positions into war options as a matter of course. The chapter's definition, applied to this record, yields the book's working posture: the defender prepares for the warrior, responds to the criminal with different tools, feeds the spy to the counterintelligence discipline, and never lets the vocabulary decide the budget.

The Proxy Question

The definition's last clause - under the authority of a political actor - carries the field's hardest practical problem, and it deserves its own section rather than a footnote. States rarely attack as themselves. The networked spectrum rewards deniability, so the state's hostile work is routinely outsourced: to contractors who sell operations the way consultancies sell advice; to criminal groups whose activities the state tolerates in exchange for occasional service; to patriotic volunteers who are encouraged, steered, and supplied while remaining formally independent; and to front organizations that hold the infrastructure. The proxy is not an anomaly of the networked spectrum - proxies are as old as warfare, from privateers to mercenaries to insurgent patrons - but the network makes proxy relationships cheap to form, cheap to conceal, and cheap to deny, and the doctrine chapter will inherit the consequences. The sorting discipline handles the proxy with a single test: what can the authority actually do? A proxy the state can restrain is the state's instrument in fact; a proxy the state merely tolerates is a neighbor's crime with a border's protection; and a proxy the state cannot control is weather with a flag. The reader who applies the restraint test reads proxy conduct more honestly than the public debate, which oscillates between attributing everything the proxy does to the patron and nothing - the truth is the restraint relationship, and it is knowable in outline even when it is never admitted in public.

The proxy question also reshapes the defender's world in a way the pure state-versus-state picture obscures: the defender's most likely sophisticated adversary is often neither a state nor a criminal but a hybrid - a criminal crew

whose tooling was built by a state, a contractor whose tradecraft circulates through the market, a volunteer whose reconnaissance the state feeds. The hybrid means the defense cannot calibrate to a single adversary type: the intrusion may arrive with criminal manners and state tools, and the response plan must survive the discovery that the actor's identity was misjudged mid-incident. The definition chapter's last practical instruction follows: sort by aim and capability first, reserve the actor question for the evidence, and build response plans that do not require the actor to be known - a principle the response half of the defense chapter will need.

The Vocabulary's History

A short history of the vocabulary gives the definition its footing, because the words the field uses arrived from three different trades and still carry their old uniforms. Cyber came from control theory - the discipline of steering systems - and inherited its aura of the technical sublime; warfare arrived from the state's oldest lexicon with all its gravity intact; and the compound term was coined in the era when the state first noticed that its military's weapons, logistics, and command were all becoming software - the observation that anything that depends on the network can be attacked through it. The vocabulary's history explains its misuse: a term coined for state-on-state military concerns became the decade's word for every intrusion, because the gravity was useful - the agency that says cyber war gets a budget the agency that says network crime has to justify. The reader's defense against the vocabulary's history is the series' habit of reading claims structurally: strip the word, examine the aim, the authority, and the threshold, and the term's borrowed gravity falls away - leaving the sorting instrument this chapter has built, which is worth more than any label.

Sorting Discipline in One Table

Because the chapter has now handled impostors, proxies, vocabulary, and record, the sorting discipline deserves its summary table, spoken in prose as the series does. Crime: the aim is payment, the authority is a market, the threshold is police, and the defense is the economics - make yourself expensive, then insure the residual. Espionage: the aim is information, the authority is a state's intelligence service, the threshold is counterintelligence, and the defense is the census - know what you hold, watch who reads it, and assume the patient visitor. Vandalism: the aim is attention, the authority is a mood, the threshold is the registrar and the patch, and the defense is hygiene plus indifference, because the vandal is fed by spectacle. Gray zone: the aim is

coercion below the line, the authority is a state wearing someone else's jacket, the threshold is contested by design, and the defense is denial plus the documentation that makes the coercion visible. War: the aim is the political end itself, the authority is the state openly, the threshold is crossed and visible, and the defense is resilience plus the state's instruments. The reader holds the table as the book's front door: every later chapter deepens a row, and every incident the decade produces walks in through one of these five rows - the sorting is the diagnosis, and the defense is the treatment that follows from getting the diagnosis right.

The Threshold Perception Test

The definition's threshold clause deserves one more instrument, because the chapter promised the reader a test, and the test is the perception audit. When an incident arrives, the question what was crossed is answered differently by the three parties whose answers matter: the attacker's doctrine holds that his intrusion was calibrated espionage - below the line by design; the defender's doctrine holds that the same intrusion against his grid was preparation for war - above the line by nature; and the audience's doctrine - the allies, the market, the public - decides which reading the history books will carry. The perception audit asks two questions of any threshold claim. First, the reciprocity question: would my doctrine read this same act as war if it were done to me? States fail this test routinely - the intrusion that is research when conducted outward is aggression when conducted inward - and the failure is diagnostic, because the doctrine that cannot pass the reciprocity test is not a threshold doctrine but a convenience. Second, the effects question: what did the act actually change in the world - copies, or states? The espionage line the chapter drew - acquisition versus alteration - is the honest anchor, and the perception audit ties the two together: alteration of the world is the war register whatever the attacker's calibration, and acquisition is the espionage register whatever the defender's anxiety, and the gray zone is precisely the space where the two readings can both be argued - which is why the doctrine chapter will find the space so crowded.

The Definition as an Operating System

The chapter's closing section assembles the sorting discipline into what the reader will actually run, because a definition that cannot be operated is a museum piece. The definition runs as a four-step drill on any incident. Step one, sort the behavior: what did the intruder do - copy, deny, corrupt, position - the arsenal chapter's four verbs, which separate espionage from sabotage

from reconnaissance-in-force before any actor is known. Step two, sort the aim: payment, information, attention, or coercion - read from the behavior's profile, the way the structural reading of the record taught. Step three, sort the authority: who can order this, judged by the restraint test - the proxy section's instrument. Step four, sort the register: crime, espionage, gray zone, or war - the table's five rows, with the perception audit applied to any threshold dispute. The drill takes minutes, needs no attribution, and outputs what every later chapter needs: the response register, the budget logic, the doctrine implications, and the vocabulary to use - and the reader who runs it on the next decade's headlines will find, as this book has argued throughout, that most of what the decade calls cyber war is something else wearing war's clothes, and that the something else - which register it is, and what that register demands - is the only question that was ever worth asking.

The Reporter's Test and the Official's Test

Two practical applications close the definition's working: the tests that two different professionals run with the same instrument, because the definition's value is that it serves both. The reporter's test asks of any incident: is the war vocabulary doing work here, or is it doing marketing? - and the honest reporter finds that the war word is right perhaps once a year in most coverage, that the crime word is right most days, and that the espionage word is right more often than anyone can prove, which is precisely why the espionage register is under-reported: its events are silent, its evidence is classified, and its vocabulary is unsellable. The official's test asks of any response: am I responding to the actor, the aim, or my own audience? - and the official's honest record is that responses are frequently calibrated to the domestic political need first and the incident's register second, which the definition cannot prevent but can at least make visible: the official who must be seen acting will prefer the crime register - charges, takedowns, seizures - because it produces announcement artifacts, while the actor who actually merits the war register is precisely the actor against whom announcements are hardest. The reader who runs both tests on a week's coverage learns the definition's last gift: a working map of the decade's information ecology, in which the vocabulary of cyber war is distributed not by the incidents' nature but by the speakers' needs - the field's deepest structural fact, and the reason a book about structure must begin with a chapter about a word.

The Sorting Instrument as a Reading Discipline

The chapter's true close belongs to the reading discipline the sorting

instrument becomes when the reader turns it on the decade's steady stream of claims, because the instrument's final test is not the analyst's incident room but the citizen's news feed. The discipline runs three passes over any coverage. The first pass strips the vocabulary: remove cyber, war, attack, and breach from the sentence, and see what behavior remains - the verb left standing is the incident's true register, and it survives every edit. The second pass prices the aim: who benefits if the claim is believed - the agency seeking a budget, the vendor seeking a fear, the official seeking a response, the outlet seeking a click - because the claim's distribution is a market, and the market's incentives explain more of the vocabulary than the incident ever will. The third pass checks the structure against the book: does the story name a station, a layer, a register, an authority - the elements this book has taught - or does it run on nouns alone; the structural story can be audited, the noun-story can only be felt. The reader who runs the three passes has converted this chapter's definition from a scholar's taxonomy into a working immunity - the ability to read the decade's coverage of networked conflict without absorbing its inflation - which is, in the end, why the book began with a chapter about sorting impostors: because the first defense any reader can run is the one between the ears, and it is the only control in the entire catalog that improves with use.

The Page to Keep

Cyber warfare is organized hostile action through or against information systems, aimed at coercing a political community, under political authority. Its impostors share its tradecraft and differ in their aims: crime wants payment and therefore has a monetization surface to attack; espionage wants copies and therefore leaves the world intact - until the same access is reused for alteration; vandalism wants attention; the insider wants no intrusion at all. Most state conduct lives in the gray zone between espionage and war, because coercion is cheapest below the target's threshold of response. At the moment of intrusion the defender often cannot tell which actor is inside, so the working rule is to defend against the worst case and let the aim reveal itself in the actor's own time. The definition is a sorting instrument, a pricing instrument, and a doctrine instrument - and the rest of the book is its working out.

ABOUT THE AUTHOR

Aiman JoeHanz writes the Building of Tomorrow series -- structural, vendor-neutral guides to the technologies reshaping industry, labor, and daily life. Each volume treats one technology the way an engineer treats a machine: definition first, then anatomy, failure modes, principles, build, deployment, and the honest decade ahead.