

The Shrinking Perspective

Joe Myers

2026-09-08

These are reading notes on two books by Henry Kissinger, thirteen years apart, and on a third, from 1957, that sits behind both. Every claim is Kissinger's unless I mark it as mine.

The shrinking perspective

In *DOES AMERICA NEED A FOREIGN POLICY?* Kissinger argued that the era of communicating by television and computer pushes policy makers towards a “shrinking perspective” (Kissinger 2001).

I read that as an inability to see the big picture. News now arrives instantly and in a form you feel before you have thought about it, and it draws reactions far stronger than print ever did. The depictions of suffering in Gaza are the plain case: the image reaches the public and the minister in the same second, and both are asked to answer for it at once.

Policy makers are led to wait for events to unfold, or to be “distracted by their echo in the media”. At the same time the line between foreign and domestic policy is being rubbed out, and the two are not one craft. Foreign policy asks for “the management of nuances in a continuous process”. Domestic policy is the work of reconciling competing interests and turning them into legislation.

The tension is about time. Diplomacy needs “the willingness to persevere through a series of steps, each of which is inevitably incomplete in terms of the ultimate goal”. Governing is judged by “achievements in shorter time frames” that are far more clearly drawn. Andy Burnham’s buses are the type of the thing: a promise you can photograph, on a deadline a voter can check. The implication is that blurring the two, or letting the second swallow the first, hamstring a foreign policy that ought to rest on strategic reflection.

Kissinger was writing in 2001 about television and the early web. The shift since has been away from broadcast and print towards PLATFORMS that carry news as one item in a feed of everything else.

Who survives a shortening cycle

Kissinger describes a vulnerability. Others have made a method of it. Steve Bannon’s rule for handling the press — “the real opposition is the media and the way to deal with them is to flood the zone with shit” — is not aimed at persuading anyone. Fire out enough truths, half-truths and lies together and no reporter can hold one controversy in view long enough to shape it, and the policy that matters goes through under cover of the noise.¹

If Kissinger is right that policy makers already wait for the echo, then flooding the zone is the deliberate manufacture of the echo. The vulnerability he named in 2001 had become a technique.

¹The boxing version: a fighter throws a chaotic barrage of jabs and feints, most meant to miss or land light, not to score but to overload. Each fake drains attention. When the guard has widened and the senses have saturated, the planned punch lands, because the opponent has been watching the flurry.

There is a further step, and it is mine rather than Kissinger's. Politicians are not free agents standing above the interests that raised them; they are expressions of those interests. The selection is structural, not conspiratorial. Break the rules of accumulation badly enough and you are removed without anyone threatening you: funding dries up, the press turns, a better-aligned challenger appears. Now add the media environment Kissinger describes, and the filter tightens again. The politician who survives is the one who performs well inside a shortening cycle — and performing well in a short cycle is not the same skill as the strategic reflection Kissinger wants, nor does it select for it. That is what the degeneration of a political elite looks like from the inside: not stupider people, but a selection mechanism rewarding a different and shallower competence.

New concepts for a new domain

WORLD ORDER grapples with the dilemmas of an order traced back to the balance of power between forces now of continental scale. Its reflections on armed conflict and on the formation of political elites are brought up to date for two things that did not exist when Kissinger began: CYBERWARFARE, and the irruption of social media as the medium of political communication (Kissinger 2014).

In addressing the link between cyber technology and world order, Kissinger picks up a thread he began almost sixty years earlier in *NUCLEAR WEAPONS AND FOREIGN POLICY* (Kissinger 1957). There the aim was to find the concepts that would keep political decision makers in control of strategy under DETERRENCE, against a doctrine of MASSIVE RETALIATION so rigid that it left a president nothing to do about a small war except begin a very large one. In *World Order* the task is to stretch that frame to the novelty of conflict in cyberspace.

So the goal is to give decision makers tools that stop them being paralysed in this space. I suspect this is also where Kissinger's own illusion sits: the belief that a balance can always be struck, if only the craft of diplomacy is equal to it.

The leap that needs new words

Kissinger's argument for why cyberspace is different rests on a claim about every earlier technology. Change over the centuries combined and refined instruments that already existed:

Even radical innovations could over time be fitted within previous tactical and strategic doctrines: tanks were considered in terms of precedents drawn from centuries of cavalry warfare; aeroplanes could be conceptualised as another form of artillery, battleships as mobile forts, and aircraft carriers as airstrips. For all their magnification of destructive power, even nuclear weapons are in some respects an extrapolation from previous experience.

The leap that needs new concepts lies instead in the “rate of change of computing power” and the “expansion of information technology into every sphere of existence”. Advanced processors “can now be embedded in almost any object — phones, watches, cars, home appliances, weapons systems, unmanned aircraft, and the human body itself”. This is the INTERNET OF THINGS.

Figure 1 gives the rate he means: the transistor count of each processor that set a new record, from the first microprocessor in 1971 to 2017 (Barentsen and Peek 2014). It rises by a factor of about eight million. The vertical scale has to be logarithmic, because on a straight one every point before roughly 2005 would lie flat along the floor.

His phrase “embedded in almost any object” invites a picture of chips getting steadily smaller, and the same data says otherwise. Over those forty-six years the process those record-setting parts were printed on shrank a thousandfold, from ten micrometres to ten nanometres. The ceiling on chip area rose. The Intel 4004 of 1971 covered twelve square millimetres of silicon; the 32-core AMD Epyc of 2017 covered seven hundred and sixty-eight, sixty-four times more. Figure 2 sets the two measures side by side.

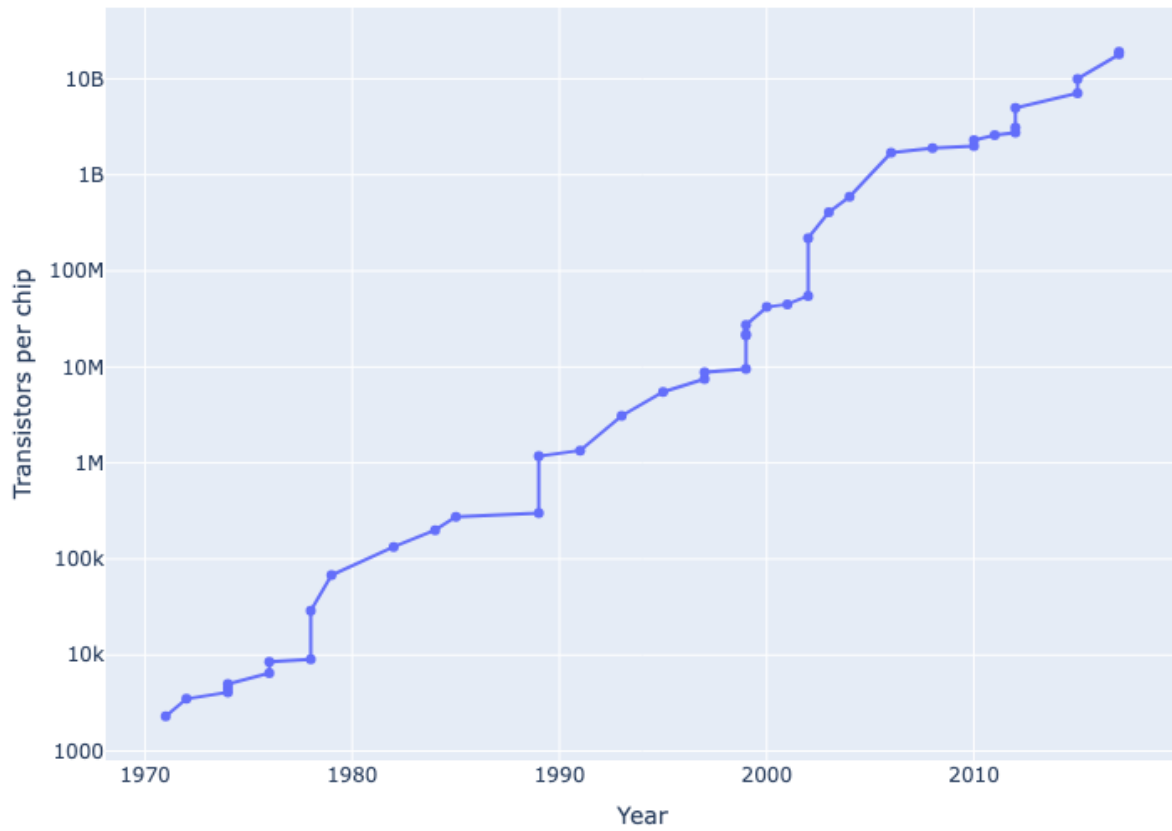


Figure 1: Every processor that set a new transistor record, 1971 to 2017 — not one reading per year: some years set several records and twenty set none. Note the logarithmic scale.

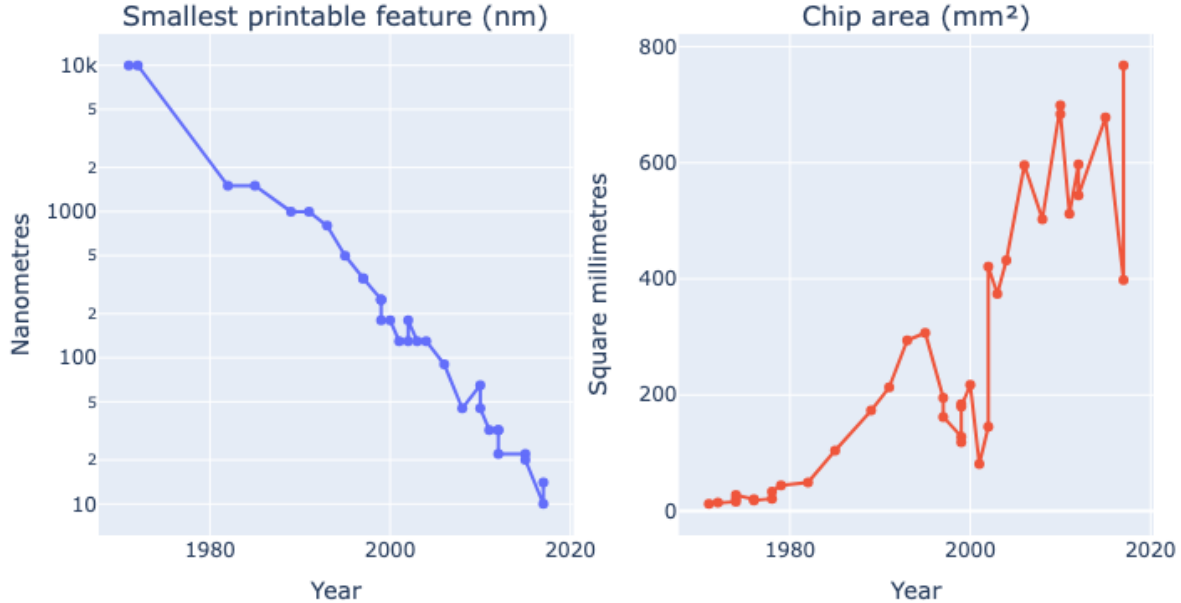


Figure 2: The two measures of size: the smallest printable feature (left, logarithmic) and the area of the chip itself (right, linear). The vertical scales differ, so the two slopes cannot be compared by eye. Each point is the process node of that record-setting part, not the finest process available that year — which is why the line occasionally rises.

So what put a processor into a doorbell was not the chip becoming small. It was transistors becoming almost free, while the chips carrying them grew. A caution about the evidence: every part in Figure 1 and Figure 2 was chosen for holding a transistor record, so they are the largest chips of their day. The doorbell’s own processor — a few million transistors on a few square millimetres — is not in this data at all. That cost series is the one I most wanted and could not source; see the section at the end.

Cyberspace colonises physical space

The revolution in handling data has for the first time brought people and processes into one medium, and “tracked their actions in a single technological language”. CYBERSPACE, a word coined in the 1980s for something that did not yet exist, “has colonised physical space and, at least in major urban centres, is beginning to merge with it”.

That merging is the whole of the internet of things, and it is what makes cyberspace a more potent ground on which to hurt an adversary. So long as a network held only information, an attack on it destroyed information. Once the network holds the valve, the dose and the signal, an attack on it destroys those. What matters is not the number of computers but the number of ordinary objects that have become computers, and I have no count of those I am willing to print: the published figures are vendor forecasts on incompatible definitions, and the best known of them — fifty billion devices by 2020 — did not happen.

Everything becomes data

Two points in this space communicate at the “near instantaneous” speed of light. Activity that a generation ago was manual or done on paper now passes through computers, and has migrated from physical space to cyberspace: “Reading, shopping, education, friendship, industrial and scientific

research, political campaigns, finance, government record keeping, surveillance, military strategy.”

All of it becomes data inside one system, quantifiable and analysable. A person with a smartphone holds information and “analytical capabilities beyond the range of many intelligence agencies a generation ago”.

Powers exceeding those of states

Here is the claim these notes are really circling. The technology groups that collect and work on the data these individuals exchange “wield powers of influence and SURVEILLANCE exceeding those of many contemporary States”, or of still more traditional powers — by which, I take it, he means the churches.

The word surveillance is doing heavy work and deserves unpacking. It means watching people systematically in order to know what they are doing, and from that to anticipate and shape what they will do. The older form is the state’s: the file, the census, the opened letter. The newer form is commercial and is rarely called surveillance at all, because its stated purpose is to sell things. But a firm that can tell from a change in a woman’s shopping that she is pregnant, before she has told her family, is doing the same work under another name. Prediction at that resolution is not a lesser thing than watching. It is what watching was always for.

The comparison with the churches is the one I most wanted to draw as a chart, and it is the one I have decided not to draw. Two objections defeat it. The first is that “power” is not a measured quantity on either side: religious affiliation is what a person says about themselves in a survey, while a platform’s user count is a number the firm produces about its own product, on its own definitions, with a commercial reason to make it large. Putting the two on one axis silently equates them. The second is the denominator: church figures are shares of a national or world population, platform figures are shares of the connected population, and a rising line crossing a falling line would encode a story about substitution that neither series tests. There is a third, blunter problem. Affiliation is falling in Britain while the number of baptised Catholics worldwide is rising, so any chart reading “religion down, technology up” has quietly chosen one country for one institution and the planet for the other.

What survives is better made in prose, and it is a sharper point than the chart would have been. Assess an institution the way you would assess the Catholic Church: by the manpower it commands, by whether its roots are global, and by whether it holds a long view of historical processes. On the first two the platforms now score as the Church does. On the third they do not, and that is the interesting asymmetry rather than an embarrassment for the comparison.

The mechanism rhymes more closely than the totals do. Confession and the feed both work by drawing out disclosure and shaping conduct through it. But confession’s knowledge was volunteered under a rule of secrecy that forbade its use, was not kept in a searchable form, and was never pooled across penitents. Platform collection is involuntary in practice, permanent, searchable, and pooled — and the pooling is exactly where its value lies. The two are alike in mechanism and unlike in retention, aggregation, and who benefits. That difference is the argument.

Private hands on a public function

Watching is one of the functions of the state, though private bodies licensed to do it are nothing new. The Pinkerton National Detective Agency is the sharp historical case: a private firm running informers and compiling files, hired by employers against organising workers, doing work that looked like policing without being answerable as police.

What has changed is scale and direction. The platforms have come to hold powers of watching that belonged to states, and which states do not possess on anything like that scale. This is most true of the internet’s transnational character, and so of the sheer quantity of data gathered: no intelligence

service using its traditional tools could ever have reached such a volume of material on the citizens of other countries, now accumulating in private servers as a by-product of selling things.

Two qualifications, both mine. There is plainly an arrangement between these firms and the state, and calling the data purely private overstates the separation. And the flow runs both ways: agencies have bought commercially collected data that they could not lawfully have gathered themselves, which turns a shopping record into an intelligence product without anyone passing a law.²

The erosion of the state as public power

The first consequence of all this concerns the MONOPOLY OF FORCE, if we count watching as one of its specific forms, and with it the character of THE STATE AS PUBLIC POWER.

Both are undermined not by the technology but by the fact that large private concentrations, owning that technology, have come to hold data on users — on citizens — at a scale without precedent, inside and beyond the borders of any state. The separation of public power from private hands is the thing being worn away. Not by a seizure, and not by anybody's decision, but as a by-product of commerce.

What the vulnerability looks like

The question takes on more weight once you consider the military implications, offensive and defensive, of being able to act in cyberspace. The following are illustrations, not forecasts, and their point is that the damage in each comes from dependency rather than from any cleverness in the intrusion.

A city's water treatment works runs its chemical dosing from a controller that was connected to a network so that engineers would not have to drive out to it. The failure is not that someone can reach the controller. It is that nobody has decided what the plant should do when it cannot trust its own readings.

A shipping line loses the systems that tell it which container is on which vessel. No ship is damaged and no port is attacked, yet the terminals stop, because a container nobody can identify cannot lawfully be released. The cargo is physically present and administratively invisible. This one is barely hypothetical: it is what happened to Maersk in 2017.

A hospital group finds that its diagnostic imaging, its drug cabinets and its staff rota all depend on one supplier, bought separately over a decade by different managers, none of whom was choosing a single point of failure.

Most quietly of all: the timing signal from satellite navigation, which synchronises electricity grids and timestamps financial trades. Almost nobody outside those industries knows the dependency exists, which is precisely what makes it worth naming. A vulnerability that is understood gets budgeted for. A vulnerability nobody has noticed does not.

The common thread is Kissinger's, and it is why he thought new concepts were needed. In each case the harm is not proportional to the force applied. That is the property the old vocabulary — cavalry, artillery, forts, airstrips — has no word for, and it is why a strategy built on GRADUATED RESPONSE has nothing obvious to graduate.

Sources still needed

These notes are unfinished in specific ways, and it is better to name them than to let them pass.

Two figures have been cut rather than published on invented numbers. One would have shown where adults in Britain get their news. It needs Ofcom's annual "News consumption in the UK", whose

²This is the passage in these notes I am least willing to publish without checking. The documented cases are real and citable, but I could not reach the documents from here.

2018 change of method means no single line may be drawn across that year, and whose report is published in a form I could not read. The other would have counted the ordinary objects that have become computers. Nobody publishes that count on a stated basis: this is the field that produced the widely repeated forecast of fifty billion devices by 2020, which did not happen, and the size of the miss depends entirely on whether telephones and laptops are counted as things. Both claims are still made above, in prose, on my word alone.

One series is missing altogether: the falling cost of computation, which is the real explanation for processors turning up inside doorbells. Nordhaus's "Two Centuries of Productivity Growth in Computing" is the standard treatment.

Two claims in the text rest on documents I have identified but not read: the purchases of commercially collected data by state agencies, and the scale of government requests to the platforms. The sources exist and are official. They are not yet cited here, so the passage stays hedged until they are.

Finally, the quotations. They are reproduced as they were drafted and have not been checked against the printed page. One phrase I did confirm against a search index appeared there with American spelling, which suggests the edition quoted here is not the New York printing in the bibliography. That needs settling before publication: the same words, the right book.

Glossary

cyberspace The connected space in which computers exchange data, together with everything now transacted there. The novelist William Gibson coined the word in his short story "Burning Chrome" (1982), where it is the brand name of a machine, and gave it the meaning we use in his novel *Neuromancer* (1984) — a consensual hallucination experienced daily by billions. It named something that did not yet exist. It has since become the ordinary medium of banking, government records, electricity supply and war.

cyberwarfare Attacks carried out through computer networks against an adversary's systems, aimed at destroying, disabling or corrupting them. Concrete cases: the Stuxnet worm, which in 2009 and 2010 drove Iranian uranium centrifuges far outside their safe speed while telling their operators nothing was wrong, and around a thousand of which were taken out of service; the shutdown of part of Ukraine's electricity grid in December 2015, where the malware opened no breakers itself — people at keyboards did; and NotPetya in 2017, which began as an attack on Ukraine and spread to shipping and pharmaceutical firms worldwide.

deterrence Preventing an act by convincing the other side that the cost of doing it will exceed the gain. It works on an intention rather than a capability, so it fails silently: you cannot tell the difference between an enemy deterred and an enemy who never meant to attack.

Does America Need a Foreign Policy? Kissinger's book of 2001, written at the close of the decade between the fall of the Soviet Union and the attacks of September 11. It asks what the United States should do with a supremacy no rival then contested, and argues that the answer needs a considered idea of the national interest rather than a run of responses to whatever the day brings. The passages used here come from its treatment of how instant communication shortens the time a government gives itself to think.

graduated response Meeting a threat with force in measured steps, each one leaving both sides somewhere further to go. The point is to keep choices open: an answer that can only be total is an answer a leader may not be willing to give, and so may not be believed. It is what Kissinger wanted in 1957 in place of massive retaliation, and it needs a scale of harms to graduate along.

internet of things Ordinary objects with processors and network connections inside them, so that they collect data and can be reached from elsewhere. A thermostat, a doorbell camera, a

pacemaker, a shipping container, a car. The phrase matters because it marks the point where an attack through a network stops being confined to information and starts having physical effects.

massive retaliation The American doctrine announced in 1954 that an attack anywhere might be answered with nuclear weapons at a place and on a scale of America's choosing. Its point was to deter cheaply. Its weakness, and Kissinger's target, was that it left a president nothing to do about a small war except start a very large one.

monopoly of force Max Weber's definition: a state is a human community that successfully claims the monopoly of the legitimate use of physical force within a given territory. Both words carry the idea. It is a claim, which is why a state that cannot enforce it is still a state; and it is over legitimate force, not all force. Everything else follows: private force is either licensed by the state or it is crime.

Nuclear Weapons and Foreign Policy Kissinger's book of 1957, written out of a study group at the Council on Foreign Relations. Against a doctrine that offered a president only the choice between doing nothing and destroying everything, it argued for limited and graduated uses of force, so that political leaders kept real choices in a nuclear crisis instead of a single unusable one. It made his reputation.

platform A company that runs the place other people's activity happens in — searching, posting, messaging, shopping, watching — and takes its revenue from knowing who did what. The word matters here because the thing it names is neither a publisher, which chooses each item it carries, nor a common carrier, which chooses none. A platform sets the rules of a space whose contents it does not own, and keeps the record of everything done inside it.

surveillance Watching people systematically in order to know what they are doing, and from that to anticipate and shape what they will do. The older form is the state's: a police file, a census, an intercepted letter. The newer form is commercial and is not usually called surveillance at all, because its stated purpose is to sell things. A supermarket that infers a customer's pregnancy from a change in her shopping, before she has told anyone, is doing the same work by a different name.

the state as public power Engels's term, from *The Origin of the Family, Private Property and the State* (1884). The state understood as force separated out from society and standing above it — an apparatus of officials, courts, police and soldiers that claims to act for everyone rather than for whoever happens to command it. What makes it public is not that it is benign but that it is set apart from private hands. The term matters here because the argument is about that separation breaking down.

World Order Kissinger's book of 2014. It reads the present through four ideas of order that grew up apart from one another — the European balance of power, the Islamic, the Chinese and the American — and asks whether anything now holds them together. Its last chapter turns to technology, and it is there that Kissinger takes up cyberspace as a domain of conflict for which the old strategic vocabulary has no words.

References

Barentsen, Geert, and Joshua Peek. 2014. *Transistor Counts*, in Tech-Progress-Data. Dataset, MIT licence, <https://github.com/barentsen/tech-progress-data>.

Kissinger, Henry A. 1957. *Nuclear Weapons and Foreign Policy*. Harper & Brothers for the Council on Foreign Relations.

Kissinger, Henry A. 2001. *Does America Need a Foreign Policy? Toward a Diplomacy for the 21st*

Century. Simon & Schuster.

Kissinger, Henry A. 2014. *World Order*. Penguin Press.