Economically Complex Cyberattacks

Scott Borg
US Cyber Consequences Unit

Most people working in cybersecurity recognize that the interconnections and complexities of our economy can have a huge effect on the destructiveness of cyberattacks. They refer casually to "network effects," "spillover effects," or "knock-on effects." Yet there is little understanding of how such effects actually work, what conditions are necessary to create them, or how to quantify their consequences.

People working in cybersecurity also generally acknowledge that combinations of cyberattacks could be much more destructive than individual attacks. Yet there is little understanding of exactly why this is the case or what the principles would be for combining attacks to produce maximum destruction.

These two sets of problems are actually the same. It is by taking account of the interconnections and complexities in our economy that cyberattackers could devise combinations of attacks to cause greater destruction. To understand how this would work, we need to look at three features of our economy that are responsible for much of its structural complexity: redundancies, interdependencies, and near monopolies. Then, as we examine these features, we need to see how each of them would prompt a different sort of attack strategy.

Economic redundancies

The first feature of our economy that's crucial to cyberattack consequences is the way systems can substitute for other systems. This is so basic to our economy that we generally take it for granted. If you can't get an airplane, you might be able to take a train. If you can't take a train, you might be able to drive a car. If you can't drive a car, you might be able to catch a bus. This sort of thing is the basis for competition and for economic choice. It means that our economy contains many redundancies.

These redundancies are usually the main factor limiting the consequences of a cyberattack. Interfering with one business system usually does little damage to the economy as a whole, because other systems simply take over that system's functions. If we diagrammed our economic activities as a giant work flowchart, connecting inputs to outputs, then the systems that can substitute for each other would be represented as parallel channels (see Figure 1a).

To deal with redundancies, cyberattackers need to employ combinations of cyberattacks designed to produce Intensifier Effects. These are simultaneous attacks on different systems or businesses that could otherwise serve as substitutes for each other. When several systems could serve as substitutes, a successful cyberattack on the first of these systems will generally have extremely limited consequences. It might be painful for the owner of that system, but the effect on the larger economy will usually be negligible. Further successful attacks on further systems that can substitute will produce only very small increases in destructiveness. This will continue until the capacity of the remaining systems is no longer enough to allow them to take over for the systems that have been attacked. When this point is reached, there will no longer be adequate substitute systems available. The consequences of the cyberattacks will then go abruptly from being small to being huge.

This has important implications for the planning of almost any cyberattacks. If the cyberattackers know what they are doing, they won't expend very much effort on attacking a system unless they can also attack the systems that could substitute for that system. Economic redundancies, and the potential for Intensifier Effects to overcome them, will be a major consideration in choosing targets.

Economic interdependencies

The second feature of our economy that's crucial to cyberattack consequences is the way production is organized into value chains. One company will turn ore into metal. Another company will turn the metal into mechanical parts. Another company will incorporate the mechanical parts into airplanes. This sort of thing is the basis for economic cooperation and high productivity. It means that our economy contains many interdependencies.

These interdependencies provide

enormous opportunities for cyberattackers, but ones that are not always easy to exploit. The reason is that the mechanisms companies employ to coordinate their value chains can also be used to make compensating adjustments if part of the value chain is disrupted. In our giant flowchart diagramming our economic activities, the systems that make up value chains would be represented as channels that flow into each other (see Figure 1b). The auxiliary systems by which companies exchange and acquire information on each other's activities are systems for adjusting the flows.

To exploit value-chain interdependencies, cyberattackers need to employ combinations of cyberattacks specifically designed to produce Cascade Effects. These are attacks on business operations that are highly interconnected and interdependent, so that interfering with one interferes with another, which interferes with another, and so on. By this mechanism, a successful attack on one set of businesses will affect numerous other businesses up and down the value chain.

In practice, a Cascade Effect almost always requires a combination of attacks. One reason is that there is usually at least a little bit of redundancy in the channels that connect value chains. Another reason is that, in addition to causing a sudden drop or rise in demand, cyberattackers intending to produce a Cascade Effect would usually need to interfere with the mechanisms by which the other members of the value chain compensate for a sudden drop or rise in demand. This attack strategy would prevent a sudden fluctuation from being "dampened" as it moved up or down the value chain, allowing its effects to spread much further than they would otherwise.

Economic near monopolies

The third feature of our economy that's crucial to cyberattack consequences is the way that "facilitating capabilities" are often leveraged to produce large or widespread benefits. These facilitating capabilities will often be very modest in scale, yet they will be crucial to much larger enterprises. In a great many cases, one or two companies will be supplying the same kind of unique or patented process to an entire industry. In the case of airplanes, for example, there are numerous situations in which a single company, with perhaps only one close competitor, will supply critical parts, manufacturing equipment, or technical services to all of the major airplane manufacturers. This sort of situation can be found in virtually every high-tech area of our economy and in many other areas as well. It is generally a consequence of innovations putting one company well ahead of the competition and of the way we reward innovations with things like patents. It means that our economy contains many functions where there are near monopolies.

The presence of near monopolies, scattered throughout our economy, gives cyberattackers another opportunity to cause massive damage. Because near monopolies produce large effects with limited means, they give attackers opportunities to produce limited effects with limited means. If we return to our giant flowchart of economic activities, each near monopoly would be represented as a point at which numerous channels radiate out to connect with many other channels (see Figure 1c).

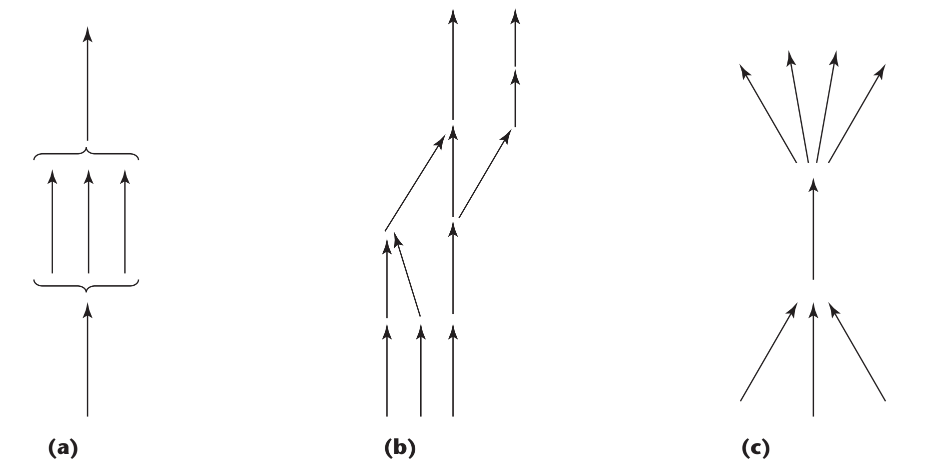

Figure 1. Economic complexities are usually due to (a) redundancy, (b) interdependency, and (c) monopoly.

To take advantage of near monopolies, cyberattackers need to employ combinations of cyberattacks specifically designed to produce Multiplier Effects. These are attacks on those business operations that are already leveraging a facilitating capability to offer large or widespread benefits with limited means. Multiplier Effects are different from Cascade Effects because they don't depend on chains of interdependencies extending their impact beyond the target company and its immediate customers. Like Cascade Effects, however, Multiplier Effects usually require combinations of attacks. This is because companies usually protect themselves from being too directly dependent on a single supplier by arranging for a second source or some buffer mechanism.

The sort of companies that could be attacked to produce Multiplier Effects would make especially tempting targets, because they tend to be small to mid-sized. This generally means that their budgets for cy-

Table 1. Complex cyberattacks.

BASIC SOURCES OF ECONOMIC COMPLEXITIES	WAYS IN WHICH COMBINATIONS OF CYBERATTACKS CAN EXPLOIT THESE ECONOMIC COMPLEXITIES
I. Redundancies Systems that can substitute for other systems by performing similar functions	I. Intensifier effects Simultaneous attacks on different systems or businesses that could otherwise substitute for each other
II. Interdependencies Value chains in which one business activity feeds into another business activity	II. Cascade effects Attacks on business operations that are highly interconnected and interdependent, so that interfering with one interferes with another, which interferes with another, and so on
III. Near monopolies Situations in which one or two companies provide the same essential product or service to an entire industry	III. Multiplier effects Attacks on the business operations that already leverage a facilitating capability to offer large or widespread benefits with limited means

bersecurity are small and their defenses relatively unsophisticated.

Quantifying economic effects

The best way to estimate the quantitative, economic effects of these complex cyberattacks is to see how they affect the transformation of inputs into outputs. Whether the attack affects a group of parallel businesses, a value chain of interdependent businesses, or a set of near monopolies that directly affect a much larger group of businesses, it is possible in each case to draw an imaginary circle around the affected business activities.

The inputs to this circle of business activities will be the potential benefits that are lost or consumed in the process of carrying out these business operations. The outputs from this circle of business activities will be the benefits gained. If the cyberattack has damaged this collection of business activities, then it will have increased the value of the inputs, or decreased the value of the outputs, or both.

We can measure the value of the inputs and outputs by seeing how they are regarded by the suppliers and the customers. For each input, the supplier will have an Opportunity Cost. This is the amount that the supplier could have gained by doing something else with the same resources. It is the supplier's "indifference point" when deciding whether to do the deal that would let those resources be the inputs for this business activity. If a supplier is offered more than its Opportunity Cost for those resources, then that supplier will generally be willing to do that particular deal. If the supplier is offered less, then the supplier would be better off doing something else.

In a similar fashion, for each output, a customer will have a Willingness-to-Pay. This is the amount that the customer would need to pay to gain an equivalent benefit from another source. It is the customer's "indifference point" when deciding whether to do the deal that encourages this product to be the output of this business activity. If a customer is offered that product for less than its Willingness-to-Pay, then that customer will generally be willing to do that particular deal. If the customer is offered the product for a higher price, then the customer would be better off doing something else.

These valuations of inputs and outputs give us a rigorous way of assessing the economic consequences of a cyberattack. The total value created by any business activity is the Willingness-to-Pay of the customers minus the Opportunity Cost of the suppliers. This is the margin by which the benefits gained exceed the benefits forgone. The total value destroyed by a cyberattack is the value created by the affected businesses without the attack, minus the value created by the affected businesses with the attack.

Implications of economics for future cybersecurity

The actual scale of damage done by cyberattacks depends overwhelmingly on the degree to which they can create Intensifier, Cascade, and Multiplier Effects. Each of these effects has the potential to expand the circle of affected businesses far beyond those businesses that are directly attacked. Each of these effects has the potential to turn relatively unsophisticated, small-scale attacks into major threats with major consequences. This means that the most important variable determining the destructiveness of future attacks will not be the technical devices used to carry them out, but the way economic structures are taken into account in the choice of targets.

The implications for cybersecurity research and development are considerable. If a hostile organization wants the ability to inflict large-scale damage by cyberattacks, it will want to devote some of its resources to new techniques for circumventing cybersecurity technology. But it will increase its destructive capabilities much faster by using its resources to investigate the economic structure of its potential targets. Being able to map the redundancies, interdependencies, and near monopolies in an adversary's economy is a more important cyberattack capability than knowing additional intrusion techniques. Even if the target is as narrow as an individual company or industry, understanding exactly how that company or industry creates value is vital to planning an effective attack on it.

If the structural analysis of an economy is a powerful tool for cyberattackers, it is an even more essential tool for cyberdefenders. An effective cyberdefense can't be satisfied with identifying a few individual cyberattack scenarios that would be highly destructive. An effective cyberdefense needs to take account of all the possible cyberattack scenarios, so that it can determine which are the highest priorities for defense. Then it needs to assess the cost-effectiveness of each possible countermeasure, so that defense resources are deployed in a responsible way. Since the scale of damage is itself determined by economic structures, these are economic questions at every level.

Taking proper account of economics in security thinking requires some adjustments in outlook. People are used to thinking of "economics" as dealing primarily with money, and "business" as concerned primarily with making money. But this is not how we are using these terms here. The sort of economics we are applying in this analysis deals not primarily with money, but with value. Even more important, the term "business" in this context refers to any collective activities that humans carry out to create value. In this basic sense, the "businesses" that could be affected by a cyberattack would include hospitals, churches, police departments, volunteer organizations, local governments, and, indeed, any cooperative activities that take less-valued inputs and produce more-valued outputs. If we want to think analytically about how to defend these activities from cyberattacks, then economics is the natural tool.

The implications of these insights for cyberattacks will be more immediate than their implications for cybersecurity R&D. As attackers become more sophisticated, they will think less in terms of individual attacks and more in terms of combinations of attacks. As their thinking becomes more analytical, they will direct their attacks less at achieving short-term bragging rights and more at achieving larger economic impacts. Whatever their agendas, potential attackers will inevitably recognize that complex cyberattacks are a tempting way to achieve them. □

__Scott Borg__ is the director and chief economist of the US Cyber Consequences Unit, recently established by the US Department of Homeland Security. He is also a senior research fellow at the Center for Digital Strategies at Dartmouth's Tuck School of Business. Contact him at scott.borg@dartmouth.edu.

Education vs. Certification • Security Nonconformists
IEEE
SECURITY & PRIVACY
Building Confidence in a Networked World
PRIVACY ON STANDBY
Computer Society
IEEE