Many speculative investors snap up tokens just to flip them to others eager to join the race.

"All crises have involved debt that has become dangerously out of scale…"

Short memory? A false sense of novelty? The supposed intellectual superiority of the moneyed folk? People eager to pour money into business plans as thin as ether? All these elements have been present in every big speculative episode in history. Crypto assets (that's what we call them at the IMF, to distinguish them from old-fashioned currencies) appear to check all these boxes. One big element is still not clear: how much debt is involved.

Debt is what drives the "insanity born of optimism and self-serving illusion," Galbraith wrote, describing how the 18th century bubbles in the United Kingdom and France became a systemic crisis. People borrow money to join the party, because other people are making tons of money. (They must know something, right?)

Just how much money investors are borrowing to buy crypto assets is still mostly unknown, because of this market's opaque and unregulated nature and early stage of development and the seemingly minimal exposure of major banks. But leverage is clearly involved. Some crypto exchanges allow investors to borrow as much as 100 times the cash balance in their accounts. A recent poll by LendEDU, a financial education website, found that a growing number of investors use credit cards to buy coins, and then carry the balance—a risky strategy.

Some people grow ridiculously rich, while others lose the farm. Anyone who bought Bitcoin in the last two months of 2017, when the price reached almost $20,000, has been played for a greater fool. Volatility isn't the only risk. Since 2011, according to *Reuters*, hackers have stolen almost 1 million Bitcoins (worth over $9 billion in early May) from several exchanges. Of course, bubbles do happen without excessive leverage. The dot-com boom is an example. Many analysts believe that is why the ensuing recession was relatively short and mild.

"The speculative episode always ends not with a whimper but with a bang…"

Galbraith concluded that, by their nature, all bubbles end badly, triggering a period of intense scapegoating, during which those previously called geniuses are blamed, but societies usually don't recognize their collective insanity—or learn from it. The current episode may produce more of a whimper than a bang. As Bank of England governor Mark Carney noted in a recent speech, even at their peak, all crypto assets combined were worth less than 1 percent of global GDP, while tech stocks at the height of the dot-com mania were valued at close to a third of global GDP.

Can any good come of this?

The so-called South Sea Bubble hit the United Kingdom during the early 18th century. For the first time, investors were able to buy shares of companies offering new and exciting products and services, like the one that promised to develop a precursor to the typewriter.

Webvan, one of the many casualties of the dot-com bubble, offered fast delivery of groceries. Founded in 1996, it went bankrupt in 2001, after burning through more than $800 million in investors' money. In July 2000, *Fortune* called AllAdvantage "the dumbest dot-com in the world." It actually *paid* people to surf the web in return for showing them ads. It, too, folded.

The current episode may produce more of a whimper than a bang.

The typewriter, of course, turned out to be the main text processing device for more than a century. Amazon (which bought Webvan), Walmart, and many other companies now offer quick grocery delivery. Facebook made a $16 billion profit in 2017 with targeted advertising, the principle that AllAdvantage tried to develop—and without paying anyone!

Yes, many crazy ideas are thrown around during periods of financial euphoria. Some do stick. Some asset price bubbles, like the dot-com episode, are periods of creative destruction that give rise to inventions that change people's lives in a lasting way. It's too early to say whether crypto assets will have a similar impact, though the signs are promising. The problem is that, while only a few bubbles create something worthwhile, all are destructive—of value, wealth, and trust in institutions. Humanity has figured out how to innovate without euphoria. But, as Galbraith shows, it rarely learns the lessons of financial bubbles. FD

ANDREAS ADRIANO is a senior communications officer in the IMF's Communications Department.

ART: ISTOCK / 1933BKK

The Industrialization of CYBERCRIME

Lone-wolf hackers yield to mature businesses

Tamas Gaidosch

Cybercrime is now a mature industry operating on principles much like those of legitimate businesses in pursuit of profit. Combating the proliferation of cybercrime means disrupting a business model that employs easy-to-use tools to generate high profits with low risk.

Long gone are the legendary lone-wolf hackers of the late 1980s, when showing off level 99 computer wizard skills was the main reason to get into other people's computers. The shift to profit making, starting in the 1990s, has gradually taken over the hacking scene to create today's cybercrime industry, with all the attributes of normal businesses, including markets, exchanges, specialist operators, outsourcing service providers, integrated supply chains, and so on. Several nation-states have used the same technology to develop highly effective cyber weaponry for intelligence gathering, industrial espionage, and disrupting adversaries' vulnerable infrastructures.

Evolution

Cybercrime has proliferated even though the supply of highly skilled specialists has not kept pace with the increasing technical sophistication needed to pull off profitable hacks with impunity. Advanced tooling and automation have filled the gap. Hacking tools have evolved spectacularly over the past two decades. In the 1990s, so-called penetration testing to find vulnerabilities in a computer system was all the rage in the profession. Most tools available at that time were simple, often custom built, and using them required considerable knowledge in programming, networking protocols, operating system internals, and various other deeply technical subjects. As a result, only a few professionals could find exploitable weaknesses and take advantage of them.

As tools got better and easier to use, less skilled, but motivated, young people—mockingly called "script kiddies"—started to use them with relative success. Today, to launch a phishing operation—that is, the fraudulent practice of sending email that appears to be from a reputable sender to trick people into revealing confidential information—requires only a basic understanding of the concepts, willingness, and some cash. Hacking has become easy to do (see chart).

Cyber risk is notoriously difficult to quantify. Loss data are scarce and unreliable, in part because there is little incentive to report cyber losses, especially if the incident does not make headlines or there is no cyber insurance coverage. The rapidly evolving nature of the threats makes historical data less relevant in predicting future losses.

Scenario-based modeling, working out the costs of a well-defined incident affecting certain economies, produces estimates in the tens or hundreds of billions of dollars. Lloyd's of London estimates losses of $53.05 billion for a cloud service outage lasting 2½ to 3 days affecting the advanced economies. An IMF modeling exercise put the base-case average aggregated annual loss at $97 billion, with the worst-case scenario in the range of $250 billion.

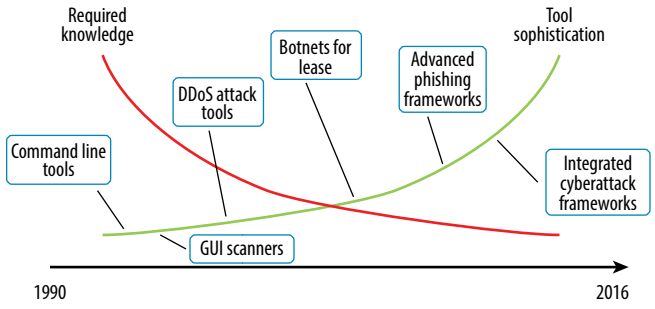
Causes and consequences

Crime in the physical world—with the intent of making money—is generally motivated simply by profit potentially much higher than for legal business, which criminals view as compensation for the high risk. In the world of cybercrime,

ART: ISTOCK/UGURHAN; VANREEEL

Child's play

As tools become more sophisticated, hacking requires less technical knowledge, and it is now much easier to pull off a hack.



Source: Carnegie Mellon University.
Note: DDoS = distributed denial of service; GUI = graphical user interface.

similar or even higher profits are possible with much less risk: less chance of being caught and successfully prosecuted and almost no risk of being shot at. Phishing profitability is estimated in the high hundreds or even over a thousand percentage points. We can only speculate on the profits made possible by intellectual property theft carried out by the most sophisticated cyber threat actors. The basics, however, are similar: effective tooling and an exceptional risk/reward ratio make a compelling case and ultimately explain the sharp increase in and industrialization of cybercrime.

Cybercrime gives rise to systemic risk in several industries. While different industries are affected differently, the most exposed is probably the financial sector. A relatively new threat is posed by destruction-motivated attackers. When seeking to destabilize the financial system, they look at the most promising targets. Financial market infrastructure is the most vulnerable because of its pivotal role in global financial markets. Given the financial sector's dependence on a relatively small set of technical systems, knock-on effects from defaults or delays due to successful attacks can be widespread, with potentially systemic effects.

Given the inherent interconnection of financial sector participants, a successful disruption to the payment, clearing, or settlement systems—or stealing confidential information—would result in widespread spillovers and threaten financial stability.

Fortunately, to date, we have not experienced a cyberattack with systemic consequences. However, policymakers and financial regulators are increasingly wary, given recent incidents that took out ATM networks and attacks against online banking systems, central banks, and payment systems.

The financial sector has been dependent on information technology for decades and has a history of maintaining strong IT control environments mandated by regulation. While the financial sector may be most at risk of cyberattack, such attacks also carry a higher risk for cyber criminals, in part because of greater attention from law enforcement (just like old-fashioned bank robberies). The financial sector also does a better job of supporting law enforcement—for example, by keeping extensive records that are valuable in forensic investigations. Deeper budgets can often lead to effective cybersecurity solutions. (A recent notable exception is Equifax, whose hack was arguably a consequence of a cyber regulatory regime that was not proportional to its risk.)

The situation is different in health care. Except in the wealthiest nations, the health care sector typically does not have the resources necessary for effective cyber defense. This is evident, for example, in ransomware attacks this year that targeted computer systems at the electronic health record company Allscripts and two regional hospitals in the United States. Although also heavily regulated and under strict data protection rules, health care has not relied nearly as much on IT as the financial sector has, and consequently has not developed a similar culture of strict IT controls. This too makes the health care sector more susceptible to cyber breaches. What is most worrisome about this weakness is that, unlike in the financial sector, lives can be lost if, for example, attackers hit computerized life-support systems.

Utilities, especially the power and communication grids, are often cited as the next sectors where large-scale cyberattacks can have severe consequences. In this case, however, the main concern is