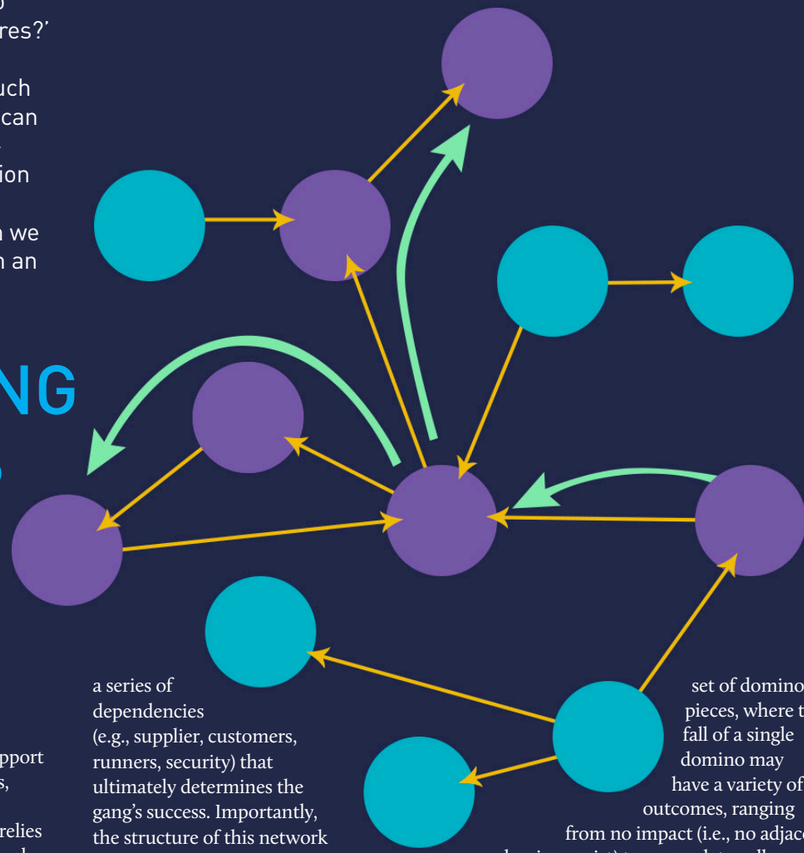
CHRISTOS ELLINAS

PREDICTING AND PREPARING FOR THE FAILURE OF COMPLEX SYSTEMS

Can Kim Kardashian's photo break the Internet? 'Who cares?' you may ask. Yet underlying this naïve question lies a much deeper and pervasive one – can a co-ordinated event single-handedly disrupt the operation of a complex system? And, importantly for security, can we predict and prepare for such an event happening?



Systemic failures

The functioning of modern society largely depends on its capacity to support the global exchange of people, goods, money and information. Similarly, organisational performance heavily relies on our ability to manage a complex web of interdependencies as they evolve throughout time, whether they correspond to material flows (e.g., supply chains), activities (e.g., projects) or interactions (e.g., teams).

It's possible to understand the various interdependencies in a system in the form of a network, where nodes and links correspond to components and their respective interdependencies. So, in the case of a drug dealing gang, the group have a series of dependencies (e.g., supplier, customers, runners, security) that ultimately determines the gang's success. Importantly, the structure of this network determines the capacity of the system to sustain large-scale, systemic failures such as the loss of a key supplier or arrest of a leading member.

The dynamics that drive these systemic failures are generally attributed to two basic mechanisms.

The first mechanism corresponds to a cascading process, where a single node fails and has the capacity to affect subsequent nodes. In search of an analogy, consider a set of domino pieces, where the fall of a single domino may have a variety of outcomes, ranging from no impact (i.e., no adjacent dominos exist) to a complete collapse (i.e., first domino in a sequence). Examples of systemic failures that reside on this mechanism include: a single task failing, ultimately affecting the performance of an entire project, or a single contaminant eventually compromising the entire supply chain. In a security context, it is akin to the discovery of one member of a cell leading to the entire group being compromised as each person leads to another.

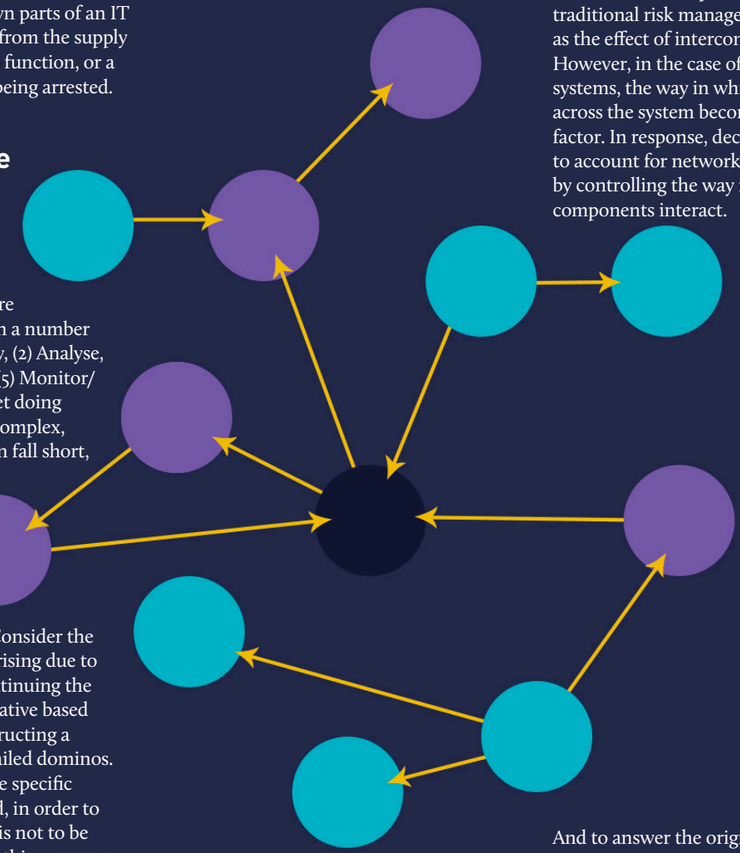
The second mechanism corresponds to the removal of individual nodes in an iterative manner. For example, consider a network where a node is selected and 'removed'. As a result, all links attached to this node are also removed, creating a 'structural hole' in the network. Repeating this process in a strategic manner can cause additional nodes to disconnect, ultimately bringing the entire system to its knees. Failures driven by this mechanism include: hackers targeting and shutting down parts of an IT system, a factory removed from the supply chain due to its inability to function, or a member of a terrorist cell being arrested.

The challenge of preventing failure spreading

In an attempt to limit the emergence of systemic 'domino' failures, risk management procedures are typically enforced, based on a number of general steps: (1) Identify, (2) Analyse, (3) Evaluate, (4) Treat, and (5) Monitor/Review all possible risks. Yet doing so in the context of these complex, interconnected systems can fall short, for at least two reasons.

First, identifying the cause of these systemic failures typically relies on narrative-based contingency approaches. Consider the case of a systemic failure arising due to the cascading process. Continuing the domino analogy, such narrative based measures focus on reconstructing a materialised sequence of failed dominos. By doing so, it identifies the specific dominos that were affected, in order to ensure the same sequence is not to be repeated in the future. Yet, this sequence is merely one manifestation out of all possible combinations allowed by the network, some of which are potentially more harmful. Hence, the risk of observing a large collapse of dominos has not been reduced, only the risk of encountering the same (or a closely resembling) one.

Second, evaluating the impact of a given risk can be exceedingly challenging. Systemic failures do not necessarily arise from large exogenous events nor require a set of extraordinary conditions. Rather, minor disturbances are sufficient in triggering both small, local and large, systemic failures. This is particularly important as the occurrence of a single node failing (or being removed) is a more probable failure scenario compared to other exotic ones.



Rethinking risk management

Network Science is helping us understand the limits of traditional risk management, along with paving new ways to account for its limitations. For example, in the case of densely-connected systems, we now know that the susceptibility to systemic failures is controlled by the stability of its individual components. In this case, traditional risk management can suffice, as the effect of interconnectivity is limited. However, in the case of sparsely-connected systems, the way in which links are spread across the system becomes a detrimental factor. In response, decision makers need to account for network effects by controlling the way in which components interact.

And to answer the original question, Kim Kardashian's photo release diverted roughly 1 percent of all internet traffic into the host webpage. Increased bandwidth requests cascaded throughout the server network, eventually slowing down the entire Internet. So in short, the answer is yes. A photo can really break the Internet.

Christos Ellinas
University of Bristol