Analyzing and Modelling the Interconnected Cyber Space[1]

H. Monsuur, R.E. Kooij and P. Van Mieghem

Chapter in 'Challenges in Cyber Warfare', Netherlands Annual Review of Military Studies 2012

1. Introduction

The security environment is rapidly changing. Due to increasing dependency on complex critical communication and information systems, society as a whole, but defence organisations in particular, have to rethink, redesign and adapt their defences to be able to confront the challenges of cyber warfare and crime. The literature abounds with examples of recent cyber attacks. We just mention the cyber attack on Estonia in 2007, the Distributed DoS attacks following WikiLeaks and the attack of the Stuxnet worm in Iran. These examples clearly underline the need to adapt our (defensive and offensive) strategy to these changes.

The NATO Strategic Concept highlighted the need to develop the ability to prevent, detect, defend against and recover from cyber attacks.[2] Due to the shift from platform-centric operations towards network-centric operations, the integrity and continuous functioning of its information systems must be guaranteed. The protection of these communication and information networks consists of two parts: *Prevention* of attacks and limiting their consequences and *resilience*, the ability to rapidly recover after an attack. To facilitate these ambitions, NATO will enhance *early warning*, *situational awareness* and *information sharing* among the allies.

Since the end of the Cold War the character of military operations has changed. Operations have become expeditionary in nature, combining defence, diplomacy and development. Coalitions include non-military organizations, host nation police forces, international organizations, commercial suppliers etc. All these partners, and their characteristic ways of operating, must find a place within the overall Command and Control (C2) structure. The goal is to share information by linking the disparate command and control systems. These C2 networks provide opportunities for increased (shared) situational awareness.[3] Although this shared situational awareness is one of the key success factors of Network Enabled Capabilities (NEC), it comes at a price: the vulnerability of the network to (targeted) attacks and the cascading consequences. As we move to systems of networked sensors, understanding the *robustness* and the *vulnerability* of these networks, when interconnected with C2 and other critical systems, is key.

[1] h.monsuur@nlda.nl, robert.kooij@tno.nl, p.f.a.vanmieghem@tudelft.nl

[2] NATO 2010

[3] Albert *et al.* 2001, Monsuur 2007a

In this chapter, we will illustrate the *vulnerability of networks to targeted attacks*. To this end, we will present ways to assess the *robustness* and *resilience* of networks.[4] Taking an Operations Research perspective, we examine the quantitative aspect of cyber operations, using network and graph theory, game theory, and (stochastic actor-based) simulations. Network robustness research is carried out by scientists with different backgrounds, like mathematics, physics, computer science, and biology. As a result, different approaches to capturing the robustness properties of a network have been proposed. The resulting insights into the problem may be used to develop appropriate (C2) network topologies that are optimal with respect to the defence against and recovery from cyber attacks.

2. Complex networks and Network Science

In several academic disciplines, like sociology, biology, economics, mathematics, physics, computer science, and electrical engineering, interactions between individual entities have been formulated in terms of networks. All these real-world representations of interconnected systems, relations, biological molecules, etc. are coined "complex networks".[5] Examples of complex networks are the relations between business companies, metabolic networks, food webs, networks of citations between scientific publications or of actors that have worked together on films, and distribution networks such as the blood vessels in the body, airline routes, electricity supply networks, and telecommunications networks. Also the concept of Network Enabled Capabilities (NEC) involves complex, networked systems, consisting of many components that are heterogeneous in functionality and capability.[6] The combined efforts of studying complex networks has led to a new research area, called "Network Science". The major difference with early network theory is that the topology of the network itself is considered as a "variable", rather than as a given, fixed initial input to the problem at hand (such as a shortest path computation or a network flow optimization). In the past few years, complex networks were mainly studied topologically: what is the structure and what are the relevant metrics to classify networks and to understand their properties (see Sec. 3.1 and 3.2). Recently, the research focus in Network Science shifted towards understanding the interplay between dynamic processes on the network and its underlying topology. The simplest example of dynamics or function and topology is the study of epidemics on networks.[7] Or, taking a more actor-based point of view, one may also use game-theoretic models for network dynamics to explain the emergence of specific network structures. In this approach, the behaviour of actors is viewed as a consequence of the network topology in which they are embedded (see Sec. 3.3).[8] In addition, one may use a multilayer approach, where nodes (C2 components) are part of physical, information, and social networks at the same time.[9]

The structural network approach has been fruitful due to its analytical tractability: there are several ways of expressing and measuring the relevant features of networks in terms of

[4] Robustness (Latin: robur; strength, hardiness, sturdiness) and resilience (Latin: resilientia; (1) action or act of rebounding or springing back, (2) elasticity: power of resuming an original shape or position after compression, (3) being able to recover quickly from (or resist) misfortune, shock, illness, etc.) are often used as synonyms.

[5] Newman 2003

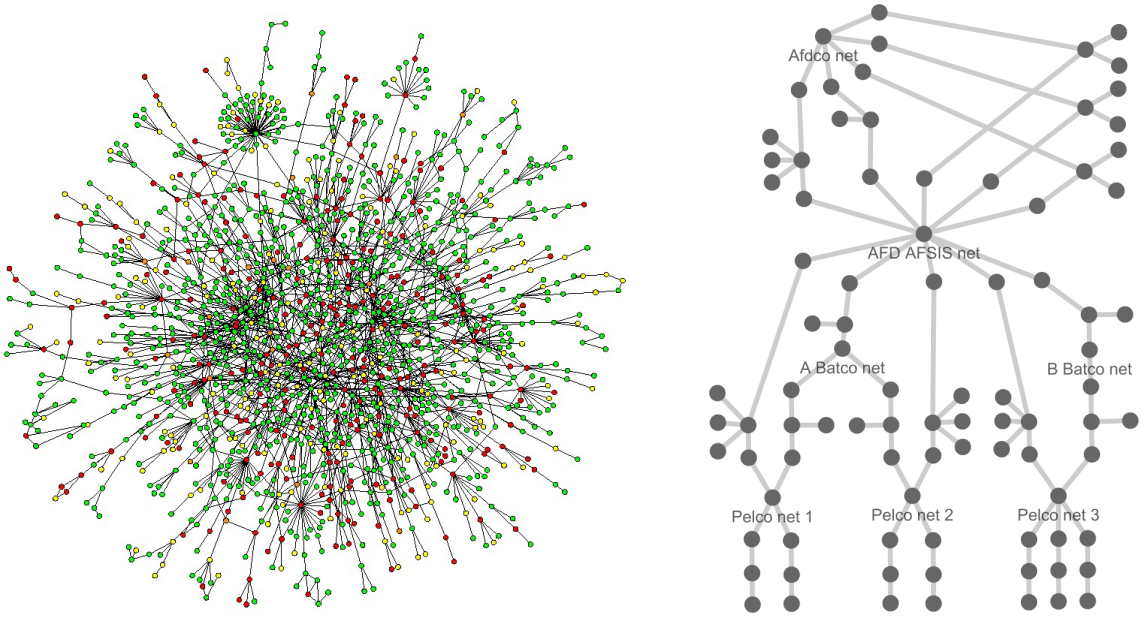
[6] Alberts *et al.* 2001

[7] See Pastor-Satorras and Vespignani 2001, Ganesh *et al.* 2005 or Van Mieghem *et al*. 2009.

[8] See e.g. Jackson and Wolinsky 1996, Jackson 2008, or Monsuur 2007b.

[9] Monsuur *et al*. 2011

topological metrics.[10] Using these network metrics, we may study the network both at the global level and at the atomic level of individual actors, using notions of centrality. In addition to the classical Erdös-Renyí (ER) *random graph* model, the Watts-Strogatz *small world* network has been introduced to account for high clustering observed in real-world networks.[11] Soon afterwards, the Barabasi-Albert (BA) power law or *scale free* graph model appeared to explain the widely-observed power law degree distribution in complex networks. BA networks are formed by the mechanism of *preferential attachment*. This means that a new node in the network will connect to already existing nodes with preference to the high degree nodes. The resulting network is characterized by the distribution of the number of links per node.[12] Fig. 1a illustrates the presence of large hubs with many connections in scale-free networks. Previous research showed that Dutch C2 networks, like for example Titaan or Afsis (see Fig. 1b), can be classified as preferential attachment or scale free networks.[13]



(a) (b)

Figure 1. (a) Network from the preferential attachment models. (b) A network representation of the AFSIS C2 network (from Grant *et al.* 2011).

Because of the existence of large hubs in scale free networks, these networks are vulnerable to targeted attacks. This will also be illustrated in Fig. 4 in Sect. 3. Moreover, the remaining network is barely able to function without these hubs. An attacker need not even know the exact location of such a hub, since most of the nodes are just a few steps away from these hubs.

[10] Examples of these metrics are the clustering coefficient, hopcount, degree distribution, betweenness, assortativity, modularity, etc. See e.g. Bocalletti *et al*. 2006 , Monsuur and Storcken 2004 or Van Mieghem *et al*. 2010.

[11] See e.g. Van Mieghem 2006a, Watts 1999. The small world phenomenon generalizes the experience that two persons that do not have a friend in common are separated by approximately less than six intermediaries.

[12] This degree distribution equals $Pr[D = k] = ck^{-\tau}$, where D is the degree of a randomly chosen node and the power law exponent τ typically lies in the range between 2 and 3, and c is a normalizing constant.

[13] Grant *et al.* 2011

These observations raise the question whether there are other network configurations that are more robust. In order to address this question we need to be able to assess network robustness.

3. Network Robustness

Network failures can be caused by either accidental or intentionally targeted attacks. Examples of accidental failures include human-made faults, manufacturing defects, worn out mechanical parts, etc. These kinds of failures appear randomly, caused by internal factors and are usually characterized as *random errors*. On the other hand, real-world systems may experience external attacks, such as terrorist or malicious software attacks, which are called *targeted attacks*.
When a network is degraded beyond an acceptable level, undesirable events may occur at any network level, such as *software malfunctions*, *security breaches*, *packet loss*, *broken links*, etc. Even assuming that all the elements of a network are equally important, the overall functionality of networked systems greatly depends on how the local elements interact with each other. Often, these constitutional parts do not operate independently, but they are connected in a complex network.[14] The failure of a single node can affect the performance of the whole network. We confine ourselves to a single network[15]. Cascading effects of random errors in interdependent networks feature first-order phase transitions (i.e. abrupt breakdown of the network when a single node is removed), whereas random errors in single networks only lead to second-order phase transitions, thus more continuous degradations when nodes are removed. The study of interdependent networks is a hot research topic, in which targeted attacks have not yet been investigated at the time of writing.

A network is connected if any node *i* in the network can be reached from any other node *j* along a path in the network. In this section, we consider a network as degraded beyond an acceptable level, if it is not connected (anymore). The aim of the first two subsections is to assess, by means of various metrics, how difficult it is to destroy the connectivity of a given network, resulting in a degraded network. This is the network robustness.[16]

A network $G(V,E)$ consists of a set of $N = |V|$ nodes connected by $L=|E|$ links. In this section, unless differently stated, we will only consider simple, undirected, connected, unweighted, finite, and deterministic networks.

3.1. Robustness related to connectivity

The node connectivity κ_v of a network is the minimal number of nodes to be removed in order to disconnect the network. The number of links that needs to be removed to disconnect the network is called the link connectivity κ_e, which obeys the inequality $\kappa_v \leq \kappa_e \leq D_{min}$, where D_{min} is the minimum degree of the vertices.[17] Both the node and link connectivity are measures for robustness, although rather coarse ones. Indeed, consider the two networks of Fig. 2: the first

[14] Boccatelli *et al*. 2006
[15] See Buldyrev *et al*. 2010 for failures in interdependent networks, such as communication networks that control a power grid.
[16] For an extensive overview of robustness measures, we refer to Grubesic *et al.* 2008.
[17] For a complete graph K_N the node connectivity cannot be determined by the definition above, because K_N cannot be disconnected by deleting nodes. The inequality $\kappa_v \leq \kappa_e \leq D_{min}$ also holds for a complete graph when its node connectivity is defined to be $\kappa_v = N - 1$. See Van Mieghem 2011.

network consists of the complete graph K_5 on 5 nodes with one extra node connected to only one node in K_5, while the second one is a tree T_5 on 5 nodes with one extra node connected to only one node in T_5. Both networks have link connectivity $\kappa_e = 1$ (remove the link that connects the extra node), but it is obvious that the first network is much more robust than the second one with respect to the removal of links.

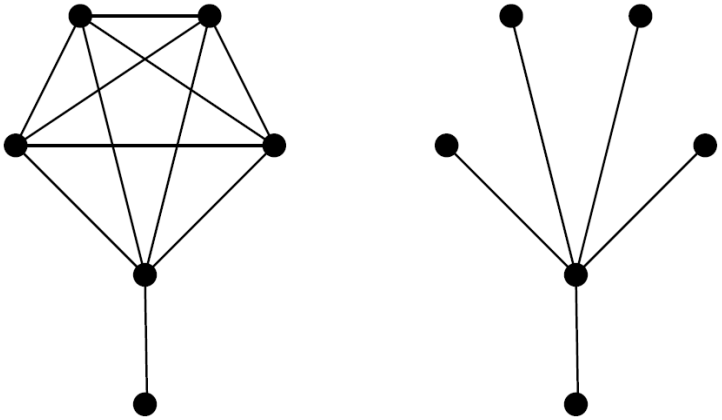


Figure 2. Two networks with same node and link connectivity, illustrating that these metrics do not capture all aspects of robustness.

Therefore, we consider a different, less intuitive class of connectivity metrics, that is related to the spectrum of networks[18]. The spectrum (eigenvalues and eigenvectors) of matrices that represent networks can be related to connectivity properties of the network. In particular, this holds for the spectrum of the so called Laplacian matrix. The Laplacian matrix Q is defined as the difference between the degree matrix Δ and the adjacency matrix A, i.e.

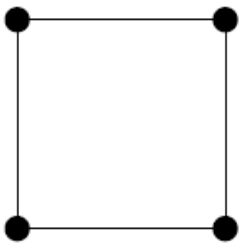
$$Q_{ij} = \begin{cases} d_i & \text{if} \quad i = j \\ -1 & \text{if} \quad (i,j) \in E \\ 0 & \text{otherwise} \end{cases}$$

where d_i is the degree (number of links) of node i.
Because the Laplacian matrix is symmetric, positive semidefinite, and the rows sum up to zero, its eigenvalues are real, non-negative and the smallest one is zero. Hence, we can order the eigenvalues and denote them as μ_i for i = 1...N such that $0 = \mu_N \leq \mu_{N-1} \leq \ldots \leq \mu_1$. The second smallest eigenvalue μ_{N-1} of the Laplacian, the so-called algebraic connectivity, has the following properties:

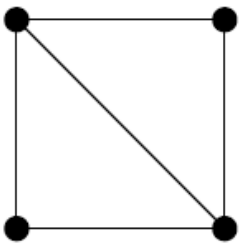
1. it is equal to zero if and only if the network is unconnected,
2. it satisfies the following inequality: $0 \leq \mu_{N-1} \leq \kappa_v$.[19]

Also this metric does not capture all aspects related to the notion of robustness, as is illustrated by Fig 3. Adding a link to the first network increases the robustness, which is not reflected in the value of the algebraic connectivity: in both cases $\mu_3 = 2$.

[18] Van Mieghem 2011
[19] Fiedler 1973



(a) $(\mu_4, \mu_3, \mu_2, \mu_1) = (0,2,2,4)$



(b) $(\mu_4, \mu_3, \mu_2, \mu_1) = (0,2,4,4)$

Figure 3. Two networks with identical algebraic connectivity μ_3 (from Baras and Hovareshti 2009).

In fact, it has been shown that in order to guarantee that a metric strictly increases when adding edges, the metric must take the *complete* Laplacian spectrum into account.[20] Examples of such metrics include the number of spanning trees and the so-called effective graph resistance.[21] The effective graph resistance *R*, also called total effective resistance or Kirchhoff index, is defined as the sum of the effective resistances over all pairs of vertices.[22] It can be written as a function of the non-zero Laplacian eigenvalues: [23]

$$R = N \prod_{i=1}^{N-1} \frac{1}{\mu_i}.$$

3.2. Robustness with respect to the removal of network elements

The last years have witnessed much research interest in quantifying the effect on the network topology, when nodes and/or links are removed from the network, either at random (failures) or targeted (attacks).[24]

A basic approach looks at the (relative) size of the largest connected component, as a fraction of the number of removed nodes, for different type of network models, such as Erdös-Renyí and scale free networks. Also different type of attack strategies are discussed, for instance based upon the degree or the betweenness of nodes. The models predict the existence of a threshold for the number of removed nodes, for which the largest component of the network disappears. For sufficiently large networks and random node removals, the formula for the critical fraction of removed nodes satisfies[25]

$$f_c = 1 - \frac{E[D]}{E[D^2] - E[D]}.$$

[20] Ellens *et al*. 2010

[21] The number of spanning trees is $\xi = \frac{1}{N} \prod_{i=1}^{N-1} \mu_i$, see Van Mieghem 2011.

[22] See Ellens *et al.* 2010. There one may also find arguments why the effective graph resistance is a suitable measure for network robustness, including a proof that the effective network resistance strictly decreases when an edge is added. Note that the smaller *R*, the more robust the network.

[23] Klein and Randić 1993

[24] See e.g. Van Mieghem *et al*. 2011b.

[25] See Cohen *et al*. 2000. An implicit formula for the critical fraction in case of attacks is given in Magnien *et al*. 2011.

Figs. 4 and 5 depict the relative size of the largest connected component for a BA scale free and ER graph with N = 100 nodes and L = 500 links, for different node removal strategies.

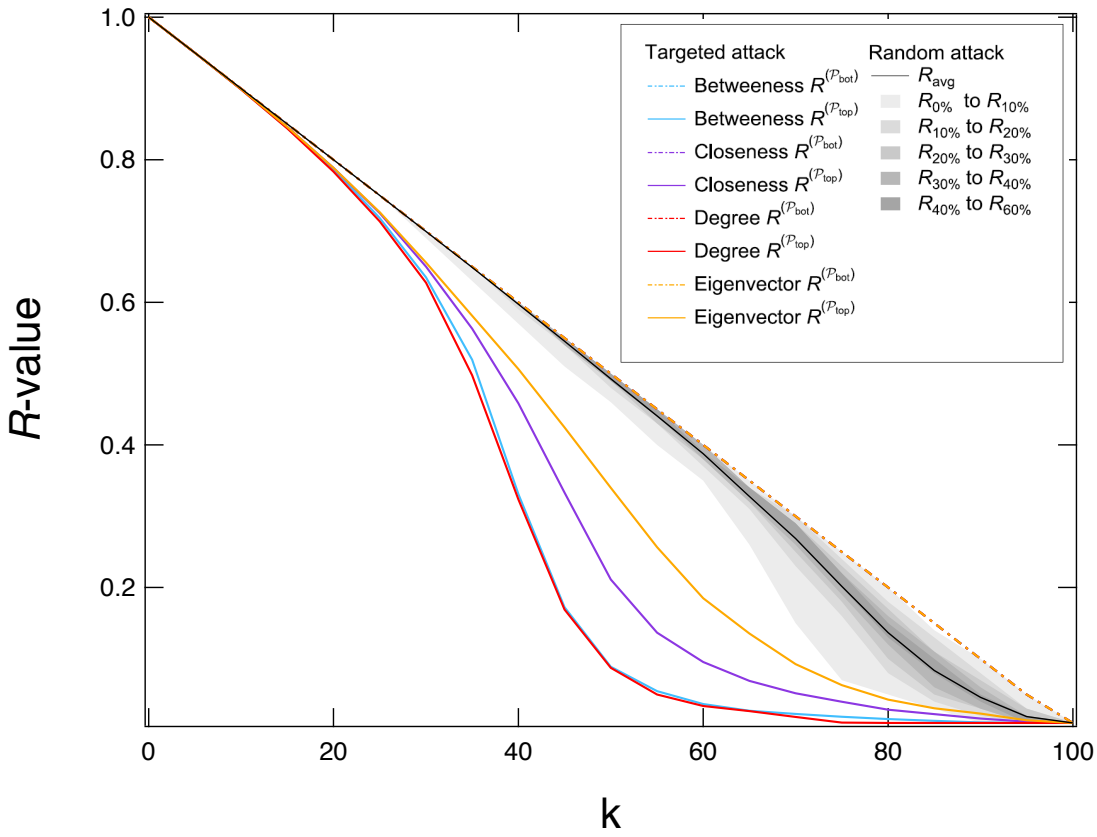


Figure 4. The *R*-value (in this case the fractions of nodes in the giant component) in a Barabasi-Albert graph (*N* = 100, *L* = 500) versus the removal of *k* nodes for different realizations of the perturbation. The set of perturbations form contour plots around the average sequence of *R*-values (from Trajanovski *et al*. 2012).

The comparison between the BA and ER graph in Fig. 4 and 5 clearly shows that the scale free networks are robust with respect to failures (shaded small area) but very vulnerable with respect to targeted attacks (large area between upper and lower R-value corresponding to the same removal strategy). Consider, for example, the situation where 40 nodes are deleted at random from the network. Then, as shown by the shaded small interval above *k* = 40, almost all of the remaining 60 nodes form a large connected component. But if 40 nodes with (for example) high degree are deleted, this largest connected component is much smaller (approximately 32). This difference between random attacks and targeted attacks is much less for the ER graphs, see Fig 5.

Recently it has been suggested not to use the critical fraction as robustness metric, but an integral measure that takes all possible numbers of removed nodes into account:

$$R = \frac{1}{N}\sum_{k=1}^{N} s(k),$$

where $s(k)$ denotes the size of the largest connected component, after k nodes have been removed.[26]

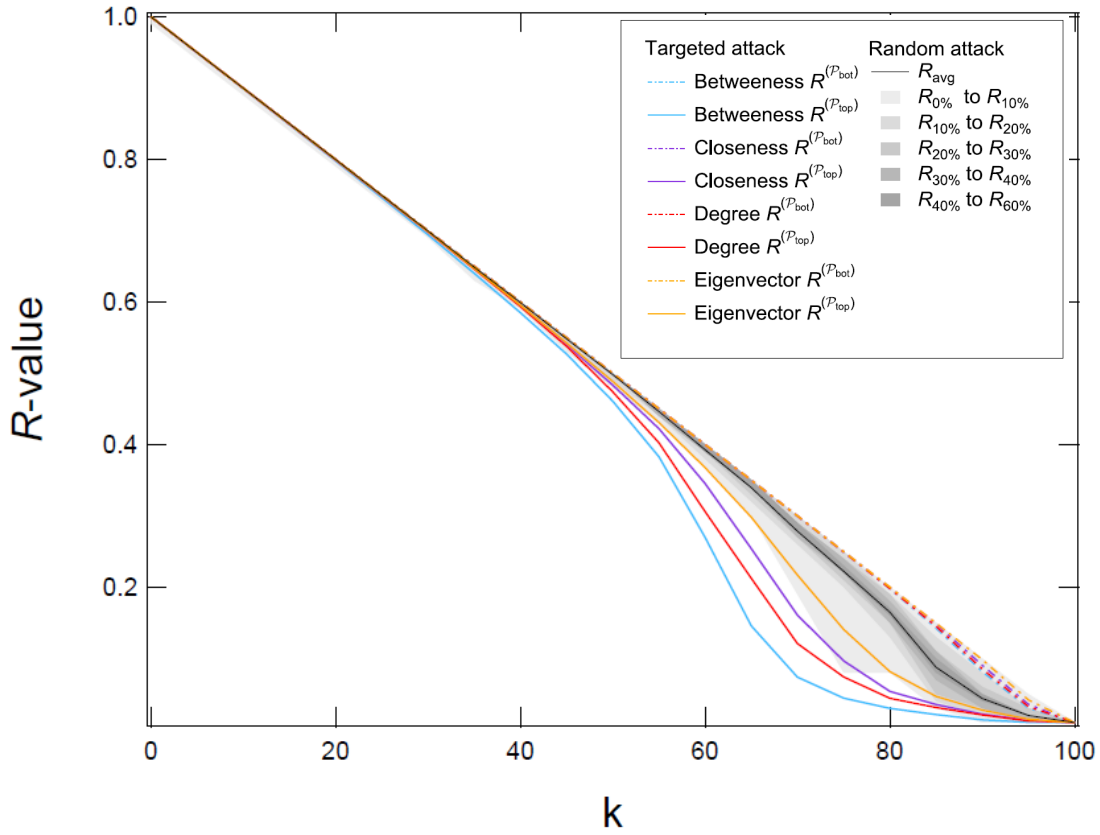


Figure 5. The *R*-value (in this case the fractions of nodes in the giant component) in a random Erdös-Renyí graph (N = 100, L = 500) versus the removal of k nodes for different realizations of the perturbation. The set of perturbations form contour plots around the average sequence of *R*-values (from Trajanovski *et al*. 2012).

3.3. The R-model

Quantifying the level of robustness of networks has been a research theme for several years. Unfortunately, there are many complications, such as a multi-layer protocol suite, different aggregation levels, missing service metrics that adequately capture and define robustness properties, and a dynamically changing and uncertain topology.[27] Most probabilistic studies assume that link failures are independent from each other and that the occurrence of each failure has a fixed, same probability p, which, although leading to nice mathematical conclusions, constitutes a major approximation of reality. These conceptual difficulties have led to the proposal of a computational framework for the topological robustness of a network.[28]

[26] See Schneider *et al.* 2011, followed by Trajanovski *et al*. 2012.
[27] See the discussion in Van Mieghem *et al*. 2010a.
[28] Van Mieghem 2010

Fig. 6 illustrates the focal question: 'Given a network at a certain time, is that network *appropriate* or *good* for its purposes?' The meaning of 'good' and 'purpose or service' need to be defined.

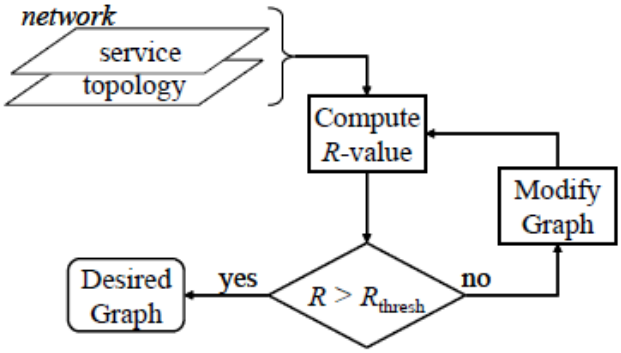


Figure 6. The flow chart of the high level goal to achieve network robustness

A given network at a certain time, defined by a service and a topology as in Fig. 6 is translated into a mathematical object, on which computations can be performed such as the computation of a 'goodness' value or robustness value, called the *R*-value. The *R*-value is a performance measure, relevant for the service and normalized to the interval [0,1], so that *R*=0 corresponds to absence of network 'goodness' and *R*=1 reflects perfect 'goodness'. The *R*-value of the network robustness is defined by a weighted, linear expression

$$R = \sum_{k=1}^{m} s_t \, t_k$$

where *s* and *t* are the *m*×1 weight and the topology vector, respectively. The components of the topology vector *t* are *m* network metrics that characterize the topology/network. For example, t_1 may represent the average hopcount, t_2 the minimum degree, t_3 the maximum degree, t_4 the algebraic connectivity μ_{N-1}, and so on. The components of the weight vector *s* reflect the importance of the corresponding topological metrics for the service. For example, real-time communication requires certain end-to-end delay bounds. The amount to which metrics influence the end-to-end delay, such as e.g. the average hopcount, the betweenness, the effective graph resistance, is reflected by the value of the corresponding component of *s*. Fig. 6 illustrates that the current *R*-value is compared with the minimal desirable value, *R_thresh*. Either the *R* -value is sufficient, in which case we refrain from taking any corrective action, or the *R*-value is too low, in which case a modification to improve the network is required.

The robustness of a network is assessed as the degree of the *network's capability to withstand perturbations during a given time interval*. An elementary change is defined as one of the five network modifications: (1) adding a node; (2) removing a node; (3) adding a link; (4) removing a link; and (5) in weighted networks, changing the link (or/and node) weight. A perturbation (e.g. either random or targeted attacks) is a series of *n* elementary network changes to which the sequence of *R*-values $\{R[k]\}_{0\le k\le n}$ can be associated. In case of (for example) the size of the giant component, (i.e. *m*=1 in the definition of *R*), almost the entire space of possible perturbations on a *single* network, thus both random and targeted attacks, has been evaluated for several

classical network models and a few real-world networks.[29] For example, Fig. 4 and 5 illustrate a typical *R*-perturbation plot (where the *R*-value is the fraction of nodes in the giant component) in a single network challenged by node removals in a large number of possible ways. The contour landscape formed by that large number of perturbations shows that the *R*-value of the particular network is reasonably insensitive to the specific nature of the perturbation since the contour plots lie in a narrow region around the average perturbation. Hence, the network, measured by this *R*-value, is robust under random as well as targeted attacks. If the contour area is large, the influence of different types of perturbations (attacks) is large and the network may be modified to withstand specific types of attacks.

3.4 Stochastic actor-based approach and resilience

Social networks and inter-alliance networks, take shape as a result of autonomous actors (the nodes in the network) seeking to achieve their individual objectives. C2 component are part of physical, information, as well as social networks. Therefore, also C2 networks are affected by the actions of individual actors.[30]

In stochastic actor-based models, actors are assumed to evaluate their network structure and try to obtain a positively evaluated network configuration of relations.[31] Possible networks that are the result of the actor's relational changes (adding or deleting a link) are evaluated by means of an objective function, which is a linear combination of several topological characteristics (effects) of the network:

$$f_a(\beta, A) = \sum_k \beta_k s_{a,k}(A) \, .$$

As in the *R*-model, the agent-based approach uses several topological properties, like average number of connections, distances, etc. But now, the evaluation may differ between the actors (the nodes). In the expression for $f_a(\beta, A)$, a is the focal actor, $\beta = \{\beta_k\}$ is a set of statistical parameters while *A* represents the possible network. Examples of topological characteristics $s_{a,k}(A)$ are the number of neighbours of an actor or the number of triads the actor is involved in, indicating some kind of local robustness. Of course, an actor will try to improve its objective function value. At each iteration, adding or removing a link is determined probabilistically using the objective function. The transition probability of changing to some new state is given by $\frac{\exp(f_a(\beta,A))}{\sum_{A'} \exp(f_a(\beta,A'))}$, where *A*' is taken from the set of networks consisting of *A* itself, together with all possible adjacency networks that can be reached from *A* by adding or deleting links. This shows that the transition process of changing from one network to another is a Markov process. It also indicates unexplained influences and limited predictability of behaviour.

Given a predefined objective function, using extensive simulations, several characteristics of the emergent network structures can be examined. Using the metrics of Sec. 3.1 and 3.2 one may investigate the robustness of the emerging networks.

---

[29] See Trajanovski *et al*. 2012.

[30] Regarding the physical network: there exist doctrines for military C2 network design, based on parameters like bandwidth, latency, etc. See Grant *et. al.* 2011.

[31] Snijders *et al*. 2010

The reverse problem, that of estimating parameters $\{\beta_k\}$ from observed emergent network structures, may be of interest to the study of *resilience*: Consider a (C2) network that has certain desirable characteristics with respect to cyber warfare. After a hostile attack, the objective function, based on the estimated parameters $\{\beta_k\}$, may be used to assure that the final emergent network has similar properties as the original undamaged network structure.[32]

An interesting topological characteristic that an actor may use to evaluate the current network structure is the covering effect.[33] A node *a* covers node *b* if all nodes linked to *b* are also linked to *a* and, in addition, node *a* has at least one extra link. Consider, for example, a node *c* that receives and transmits information from/to nodes *b* and *d*, as in Fig. 7.

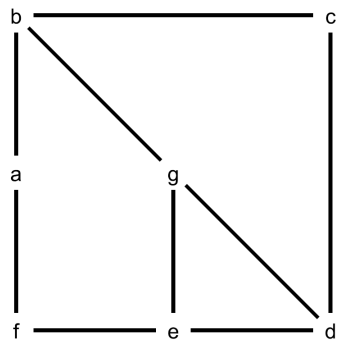


Figure 7. Example network illustrating that node *c* is covered by *g*.

The nodes *b* and *d* also are linked to node *g* which, in addition, is able to exchange information with node *e*. So, every information link of *c* can be covered by one of *g* and *g* has at least one extra information link. With respect to information sharing, distribution and processing, and robust communication possibilities, node *g* outperforms node *c*, because *g* has an additional link (to node *e*)

A special kind of network structure is a network in which each node is uncovered. We call such a network stable: no node in the (C2) network is outperformed by other nodes with respect to communication possibilities. We let $g(n,p)$ be the probability that an ER graph is a stable network. Fig. 8 draws $g(n,p)$ for several small values of n. It can be shown that $\lim_{n\to\infty} g(n,p) = 1$.[34]

[32] See Janssen *et al.* 2012.

[33] Let a and b be two nodes in V. Then a covers b in $G(V,E)$ if (1) for all $x \in V\backslash\{a\}$, $(x,b) \in E$ implies $(x,a) \in E$, and (2) there exists at least one node c different from a and b such that $(c,a) \in E$ while $(c,b) \notin$ E. See Monsuur and Storcken 2004 for axiomatic characterizations, and Janssen and Monsuur 2012 for application to terrorist networks.

[34] Janssen and Monsuur 2012

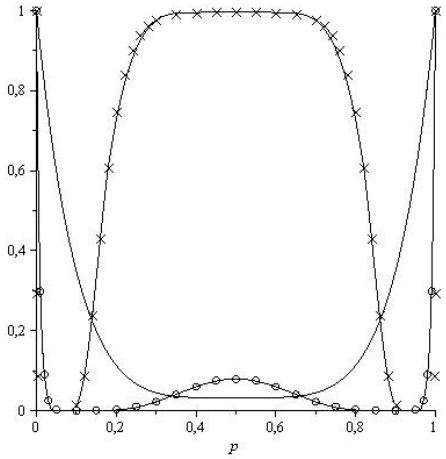


Figure 8. $g(n,p)$ as function for p for n = 5(-), 16 (o), 50 (x) (from Janssen and Monsuur, 2012).

4. Offensive Cyber warfare: Interdiction on Communication Networks

In this section, we briefly discuss interdiction policies to damage communication or C2 capabilities of adversaries. A technique that can be used to model interdiction policies is game-theoretic risk analysis.[35] Much research has been devoted to *game-theoretic risk analysis* applied to homeland security and defence. *Attacker-defender models* are used to assess infrastructure vulnerability to intentional attacks. An *interdiction model* describes an infrastructure system and its value, including how the actions of two adversaries influence this value. The two adversaries, the attacker and the operator of the C2 network, have opposite goals: while the operator's goal is to maximize the total (possible) flow of communication through the network, the attacker attempts to minimize this value. To this end, the attacker can perform interdiction actions on the network components, which change the components' communication capacity, often effectively removing the total capacity of the communication link from the network. We assume that the reduction in capacity is a linear function of the interdiction resources allocated by our interdiction forces.

Interdiction incurs a cost and we may assume that the attacker's actions are limited by a budget. Consider the simple network shown in Fig. 9. The operator of the C2 network tries to maximize the possible communication from the base *O* to the target destination *T* using intermediate communication links. The numbers c_k on the arcs indicate the maximal possible dataflow on that link *k*.

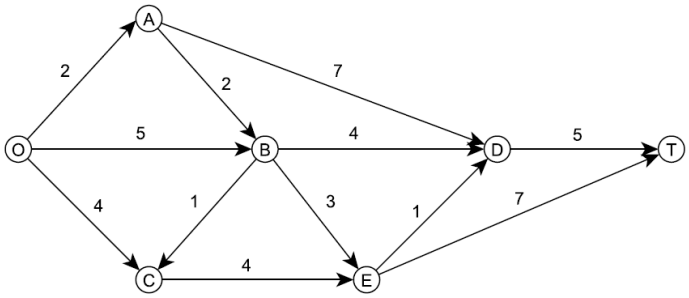


Figure 9. A (directed) C2 network.

[35] See e.g. Bier and Naceur Azaiez 2008.

If the attacker is able to interdict the equivalent of two communication links, its problem may be formulated as:

$$\min_x \max_y \quad y_{OA} + y_{OB} + y_{OC}$$

s.t.

$$y_{OA} = y_{AB} + y_{AD}$$

$$\dots$$

$$y_{BE} + y_{CE} = y_{ED} + y_{ET}$$

$$y_k \leq c_k(1 - x_k) \text{ for all links } k$$

$$\sum_k x_k = 2$$

where, for example, y_{OA} is the dataflow along the link *OA*, and x_k is a binary variable, which is equal to 1 if the link *k* is interdicted, 0 otherwise. In the literature one may find several strategies to solve this kind of min-max problems.[36]

5. Conclusions

Modern society increasingly depends on a complex infrastructure of information and communication systems. While these complex networks create new opportunities for offensive cyber warfare, they also pose new challenges to protect our networked systems against cyber attacks. In this chapter, we showed that understanding the robustness and the vulnerability of the networks, that facilitate our intertwined society or our interconnected C2 systems, is of vital importance. We illustrated various approaches to assess the robustness of networks. Several of these metrics can be implemented in doctrines for robust network design. We also focussed on the recent shift in Network Science towards understanding the interplay between the dynamic processes on the network and its underlying topology. The resulting insights may serve as a first step towards a methodological framework to defend networks against and recover from cyber attacks.

[36] Brown *et al.* 2006

References

Alberts, D.S., J.J. Garstka, R.E. Hayes, and D.A. Signori (2001). Understanding information age warfare. *US Department of Defense Command & Control Research Program*, Washington DC.

Baras, J.S., and P. Hovareshti (2009). Efficient and robust communication topologies for distributed decision making in networked systems. In: *Proceedings of the 48th IEEE Conference on Decision and Control*, Shanghai, China.

Bier, V.M., and M. Naceur Azaiez (2008). *Game Theoretic Risk Analysis of Security Threats*. Springer

Boccaletti, S., V. Latora, Y. Moreno, M. Chavez, and D. Hwang (2006), Complex networks: Structure and dynamics, *Physics Reports*. 424:175—308.

Brown, G., M. Carlyle, J. Salmero´n, and R.K. Wood (2006). Defending critical infrastructure. *Interfaces* 36, 530–544.

Buldyrev, S. V., R. Parshani, G. Paul, H. E. Stanley, and S. Havlin (2010). Catastrophic cascade of failures in interdependent networks. *Nature Letters*, 464:1025—1028.

Cohen, R., K. Erez, D. Ben-Avraham, and S. Havlin (2000). Resilience of the Internet to random breakdowns, *Phys. Rev. Lett*. **85**, 4626.

Ellens, W., F. A. Spieksma, P. Van Mieghem, A. Jamakovic, and R. E. Kooij (2011). Effective graph resistance. *Linear Algebra and its Applications*, 435:2491—2506.

Fiedler, M. (1973). Algebraic connectivity of graphs, *Czechoslovak Mathematical Journal*, 23:298-305.

Ganesh, A., L. Massoulie, and D. Towsley (2005). The effect of network topology on the spread of epidemics. *INFOCOM 2005*, 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE 2, 1455-1466 vol. 2.

Grant, T.J., B.C. Buizer, and R.J. Bertelink (2011).Vulnerability of C2 networks to attack: Measuring the topology of eleven Dutch Army C2 systems*. ICCRTS 2011* paper ID087.

Grubesic, T. H., T. C. Matisziw, A. T. Murray, and D. Snediker (2008). Comparative approaches for assessing network vulnerability. *International Regional Science Review*, Vol. 31, pp. 88-112.

Hethcote, H.W. (2000). The mathematics of infectious diseases. *SIAM Review* 42, 599-653.

Jackson, M.O. (2008). *Social and Economic Networks*. Princeton University Press.

Jackson, M.O., and J. Wolinsky (1996). A strategic model of social and economic networks. *Journal of Economic Theory* 71(1):44-74.

Janssen, R.H.P., and H. Monsuur (2012). Minimal stable network topologies using the notion of covering. *European Journal of Operational Research* 218, 755–763.

Janssen, R.H.P., H. Monsuur, and A.J. van der Wal (2012*). Emergent network Structures in Stochastic Actor-Based Modeling: The Influence of Covering.* Scientific Report of the Netherlands Defence Academy, February 2.

Klein, D.J., and M. Randic (1993). Resistance distance. *Journal of Mathematical Chemistry*, 12:81-95.

Kooij, R. E., P. Schumm, C. Scoglio, and M. Youssef (2009). A new metric for robustness with respect to virus spread. *Networking 2009*, LNCS 5550, pages 562 — 572.

Magnien C., M. Latapy, and J-L. Guillaume (2011). Impact of random failures and attacks on Poisson and power-law random networks. *ACM Computing Surveys*, Volume 43 Issue 3.

Monsuur, H. (2007a). Assessing situation awareness in networks of cooperating entities: A Mathematical Approach. *Military Operations Research*, 12 (3), 5-15.

Monsuur, H. (2007b). Stable and emergent network topologies: A structural approach. *European Journal of Operational Research*, 183 (1), 432-441.

Monsuur, H., and T. Storcken (2004). Centers in connected undirected graphs: An axiomatic approach*. Operations Research*, vol. 52 (1), 54-64.

Monsuur, H., T.J. Grant, and R.H.P. Janssen (2011). Network topology of military command and control systems: Where axioms and action meet. In: J.P. Bauer (ed). *Computer Science Research and Technology*, Volume 3: 1-27, Nova Science Publishers.

NATO (2010). http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

Newman, E.J. (2003). The structure and function of complex networks. *SIAM Review* 45, 167-256.

Schneider, C. M., A. A. Moreira, J. S. Andrade Jr., S. Havlin, and H. J. Herrmann (2011). Mitigation of malicious attacks on networks, *PNAS* **108**, 3838.

Snijders, T.A.B., G.G. van de Bunt, and C.E.G. Steglich (2010). Introduction to stochastic actor-based models for network dynamics. *Social Networks*, 32, 44-60.

Trajanovski, S., J. Martin-Hernandez, W. Winterbach, and P. Van Mieghem (2012). Evaluation of topological network robustness. Unpublished.

Van Mieghem, P. (2006). *Data Communications Networking*. Techne Press, Amsterdam.

Van Mieghem, P. (2006a) *Performance Analysis of Communications Systems and Networks*. Cambridge University Press, Cambridge, U.K.

Van Mieghem, P. (2011). *Graph Spectra for Complex Networks*. Cambridge University Press, Cambridge, U.K.

Van Mieghem, P. (2011a). The N - intertwined SIS epidemic network model. *Computing*, 93(2):147—169.

Van Mieghem, P. (2012). The viral conductance of networks, *Computer Communications*, to appear.

Van Mieghem, P. (2012a). Epidemic phase transition of the SIS-type in networks. *Europhysics Letters* (EPL), 97:48004.

Van Mieghem, P., C. Doerr, H. Wang, J. Martin Hernandez, D. Hutchison, M. Karaliopoulos, and R. E. Kooij (2010a). A framework for computing topological network robustness. Delft University of Technology, Report20101218 (www.nas.ewi.tudelft.nl/people/Piet/TUDelftReports).

Van Mieghem, P., J. Omic, and R. E. Kooij (2009). Virus spread in networks. *IEEE/ACM Transactions on Networking*, 17(1):1—14.

Van Mieghem, P., D. Stevanović, F. A. Kuipers, C. Li, R. van de Bovenkamp, D. Liu, and H. Wang (2011b). Decreasing the spectral radius of a graph by link removals. *Physical Review E*, 84(1):016101.

Van Mieghem, P., H. Wang, X. Ge, S. Tang, and F. A. Kuipers (2010). Influence of assortativity and degree-preserving rewiring on the spectra of networks. *The European Physical Journal B*, vol. 76, No. 4, pp. 643-652.

Watts, D.J. (1999). *Small World, the Dynamics of Networks between Order and Randomness*. Princeton University Press.

Youssef, M., R. E. Kooi, and C. Scoglio (2011). Viral conductance: Quantifying the robustness of networks with respect to spread of epidemics, *Journal of Computational Science*, Vol. 2, Issue 3, Pages 286–298.