National Intelligence Systems as Networks

Power Distribution and Organizational Risk in Brazil, Russia, India, China, and South Africa

Marco Cepik, PhD*
Gustavo Möller

The legitimacy and performance of intelligence services continue to be as controversial as ever. Globalization only made matters more complicated. First, more actors (including business firms, nongovernmental groups, and international organizations) are engaging in such activities with a plethora of new technological resources. Second, it has become even harder to achieve a proper balance between security and freedom in the Digital Age. Finally, as a reminder of the international anarchic structure and its political constraints, intelligence services are present in both democratic and authoritarian countries. Along with police and the armed forces, they form the core of any state's coercive power. Often, one state's intelligence success is another state's security breach. Their best-regarded mission, however, is to provide specialized knowledge about threats and vulnerabilities to the benefit of the national security decision-making process. Their internal workings, institutional interactions, and externalities are the main subjects of an interdisciplinary field of research called Intelligence Studies. This field is closely related to similar undertakings, such as Strategic Studies, Defense Studies, and the International Security subfield in International Relations and Political Science.

*Dr. Marco Cepik is an Associate Professor of International Security and Comparative Politics currently based at the Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil. He has been invited as visiting scholar by the Renmin University (RUC, Beijing), University of Oxford, Naval Post Graduate School (NPS, Monterey-CA), Indiana University of Pennsylvania, and the Latin American Social Sciences School (FLACSO, Ecuador).

Gustavo Möller, Manager, Núcleo de Estudos em Economia Criativa e da Cultura (NECCULT), Faculty of Economics, Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil

Marco Cepik and Gustavo Möller, "National Intelligence Systems as Networks: Power Distribution and Organizational Risk in Brazil, Russia, India, China, and South Africa," *Brazilian Political Science Review*, 11, no. 1 (2017), e0001. Epub 27 March 2017.https://dx.doi.org/10.1590/1981-3821201700010001.

One topic of permanent interest to Intelligence Studies is the distribution of power among the various elements comprising contemporary national intelligence systems. As pointed out by Gill and Phythian, the organizational/functional way of looking at the intelligence services has privileged the study of the United States and the United Kingdom.[1] Even so, the study of intelligence has also benefited from over 20 years of comparative research.[2] Most of the progress has been obtained on specific issues such as legislation, professionalization, external control, impact of terrorism, and democratization processes.[3] There are two main obstacles to advancing the comparative study of intelligence. The first one is empirical, as the difficulties in gaining access, dealing with disinformation, and official secrecy are even more restrictive when it comes to researching other countries. The second type of obstacle is theoretical, due to a lack of dialogue between organizational and interactional (behavioral) explanations of national intelligence systems' evolution.[4]

Therefore, the main contribution of this article is advancing comparative research in Intelligence Studies. Network analysis will be employed to assess national intelligence systems in Brazil, Russia, India, China, and South Africa. These five countries are members of the international group called BRICS, which brings together the largest developing economies in the world. Despite significant heterogeneity regarding military capabilities, threat perceptions, political regimes, diplomatic stance, and economic profiles, they are the most important states in the contemporary world along with the United States of America and its allies.[5] Although the BRICS are relevant actors on the world stage, our primary goal here is not to compare how powerful their national intelligence systems are, neither in contrast to the United States of America's intelligence community, nor in relation to each other. Instead, our task is to compare how power is distributed 'inside' each national system. Hence, we have tried to answer three questions: 01. How are the national intelligence systems organized in the five countries? 02. How is power distributed among specific organizations in each national intelligence system? 03. What are the implications of a given distribution of power to the system's overall organizational risk?

We define intelligence systems as networks composed of nodes (organizations) and links (relations), which allows us to consider the asymmetries of authority and information control as indicators of power distribution in a given network. Three types of organizations will be analyzed: supervising (government), coordinating (collegiate bodies), and executing (agencies). A fourth type of organization, namely external control bodies (control), was not included, for brevity. The empirical data from each country comes from public documents, legislation, and media news. We are aware of the limitations imposed by using such sources.

Nonetheless, graphs and adjacency matrices used in Network Analysis are better than traditional organizational charts to describe intelligence systems, because they allow for the representation of the mutual relations between the nodes of the network.[6] Moreover, once the power distribution inside the network is understood, one can begin to explain things like organizational risk, which is a range of effects from mild difficulties in achieving cooperation to severe difficulties to adapt to new strategic challenges, resulting in potential fragmentation of the network.[7]

In the next section, we explain the methods used to answer the research questions, including definitions, technical choices and procedures for data collection, calculations, results verification, and analysis of discrepancies. We then present the results obtained for each of the five countries (Brazil, Russia, India, China, and South Africa). In the final section, we compare the results obtained for each country in order to answer the research questions and to indicate limits and challenges for the next round of comparative intelligence studies.

Methods

Networks are formed by nodes (also called vertices) and links (also called edges). The nodes can be people, cities, knowledge, resources, or any material or immaterial objects one chooses to analyze. In the case of national intelligence systems, all the nodes belong to a single class, namely, organizations. As organizations are collective actors, throughout the article the terms node, actor, and organization will be used interchangeably. For a network to exist, the nodes must be linked by means of a flow or relationship. The links between nodes can be directed (indicated by an arrow) or undirected (reciprocal). For the analysis of national intelligence systems, we considered both directed links (authority) and undirected links (information flows).

By authority, we mean the hierarchical subordination exercised by an organization over another. As part of a contemporary state, even staff relationships (experts asked to provide information instead of simply being told what to do) in intelligence happen in a bureaucratic and at least partially formal setting. In turn, the information flows between organizations were assessed according to formal reporting obligations, common membership, or otherwise indicated by country specific sources. Together, authority and information flows amount to a relational definition of power.[8] In other words, power stems from the position of an actor in the network. This position is determined by the number and the intensity of subordinate relationships that the actor experiences. Moreover, the actor's position is

also determined by the number and intensity of information flows that it intermediates.

Analyzing data obtained from public documents and news, the authority exercised by each organization was rated by the authors on a scale of four intervals (0, 03, 06, and 09). The intensity 09 indicates relations provided for by law and deemed effective; that is, authority to request others to collect and analyze information or act upon it which is both legally sanctioned and carried out without any significant insubordination. Authority relationships with intensity 06 are those provided for by law, but in which there are limitations on the observed degree of subordination, either in specific subjects or time periods. A level 03 of authority is one provided by law, but characterized by significant insubordination or leeway. It can also represent a situation where the organization is legally subject to a particular actor, but informally it is another actor who effectively subordinates it. It can also express a reversal of the direction of command. We apply '0' when no relationship exists between organizations, or when it is irrelevant to the functioning of the national intelligence system.

The same scale was used to rate the intensity of information flow. Relations in which the intensity was classified as 09 are those where the information flow is provided by law and where there is evidence that it is effective between two nodes in the network. In turn, intensity 06 indicates an information flow provided by law, but ineffective for various reasons (low sharing rates, competition between agencies, administrative rules of compartmentalization, etc). An intensity 03 was attributed to information flows that are not provided legally, but in which there is evidence of its existence between two actors. We apply '0' when there is no relevant flow of information between two nodes in the network.

The primary data about intelligence services is qualitative in nature and has been acquired from public sources, such as official documents, legislation, books, articles, and news.[9] Deciding which organizations make up a national intelligence system in the case of the BRICS countries presents some difficulties.[10] When available, legal definitions determine which organizations are part of the national intelligence system. When there was no legal basis to decide on the system's components, we have used the thematic proximity of an organization to national security matters to include it or not. Thus, many organizations dedicated to criminal intelligence activities, especially at the local level, were not included in the network. Similarly, private and non-governmental organizations were excluded, even as we recognize the growing importance and the need for additional research on them.[11] Task forces, fusion centers, and working groups were also excluded from the network. We are aware of their increasing importance in many places. However, their temporary and sometimes 'ad hoc' nature makes it difficult to even

compile enough information at this point. In the case of police, military, and constabulary forces scattered throughout the territory and with very complex divisional systems, we decided to group them by functionality and subordination at the national level (see Country Results). All network nodes belong to the same class (organizations), but they were classified into three major types: supervising (government), coordinating (collegiate bodies), and executing (agencies). As mentioned before, we are still collecting data about a fourth type of organization very relevant in intelligence systems, namely external control organizations (parliamentary committees, special courts, etc).

Once the organizations that form a country's national intelligence system have been established, we have also weighted the intensity of a certain relationship between any two given organizations inside that system. For instance, the authority relationship between a collegial organization (coordination) and the other nodes of the network was classified as intensity 09 only when an organization member of the collegiate body had the power to dissolve the collegiate, combining both coordinating and commanding roles. In other cases, this type of node always had its authority relations classified as grade 06. The authority relationship of the head of state with other nodes of the governmental supervising and directing organizations (government) type were classified with intensity 09 with the exception of some cases, based on evidence and explained in the text. Finally, although task forces, fusion centers, and working groups have not been included per se as nodes in the network, their existence was considered in view of the intensity attributed to the information flow relations between participating nodes of the task force.

Once all components of a national intelligence system (the network nodes) were identified and classified, their mutual relationships were recorded in two matrices, one for the relations of authority and others for the information flows. Adjacency matrices are one way to represent a network. In them, the same actors (or network nodes) are arranged in two axes, with rows and columns forming a square. In the cells of the matrix every relationship between two actors is recorded according to their intensity scale. Obviously, diagonal cells which cut the array in half (relating each actor to itself) are filled with '0.' The matrices are the basis for recording data, generating graphs, and performing calculations.[12] All work has been carried out with the help of ORA software (Organizational Analyzer) developed by the Center for Computational Analysis of Social and Organizational Systems (CASOS) of Carnegie Mellon University.[13]

In order to answer the research question on the power distribution in each national intelligence system, two different centrality indexes were calculated for

each node. According to Brandes and Erlebach, different centrality indexes allow for the observation of different aspects of power relations in a network.[14]

The Degree Centrality index, for example, is defined as the number of links between a node and the others, i.e., how connected is a node. In directed graphs, such as those generated by the authority matrix, we have two measures of centrality, one computing relations in which the actor is being subordinated (in-degree), and other relations in which the actor is subordinating another (out-degree). Therefore, the Degree Centrality is a composite index, which can be decomposed into in-degree, out-degree, and total degree measures. The higher the relative distribution of connections a node (organization) has, the less dependent it becomes on any other specific node.[15]

In turn, the Betweenness Centrality index is obtained by computing the number of times a given node intermediates the relationship between other nodes in a geodesic path (i.e., the shortest path between two nodes). This index allows us to evaluate which nodes (actors) are in the position of stakeholders, that is, who have the power to withhold information within the network and the potential to break or prevent relations, in fact isolating other actors.[16]

First, each centrality index (Degree and Betweenness) was calculated separately for each node (organization) in the network. Then, the results were normalized on a scale between 0 and 100, thereby equalizing the size of different national intelligence systems, which is technically called the network diameter. Normalization was achieved by adding the indexes obtained for each actor and then dividing the individual index of each actor by the value of the sum of them all. Finally, the normalized indexes were compared to establish the relative position (power) of each actor in the network. Henceforth, the method combines qualitative and quantitative steps. Qualitative steps are crucial and drive the process, although deciding upon the proper indexes and providing calculations is an important part of the methodology as well.

To answer the research question concerning the organizational risk of a national intelligence system due to a particular distribution of power, two additional indexes were used, in accordance with McCulloh, Armstrong and Johnson.[17] Remember that by organizational risk we mean the probability that the system's internal power distribution will produce a range of effects from mild difficulties in achieving inter-agency cooperation to severe difficulties to adapt to new strategic challenges, resulting in potential fragmentation of the network. Unfortunately, the methodology cannot establish which effects will follow or how the respective national government will respond to such difficulties.[18] Also, it is important to notice that Network Analysis literature uses similar names for the additional indexes. Although it can be a bit confusing, just remember that while the previous

indexes were calculated for each node of the network, these two new indexes are applied to the network as a whole (graph level analysis).

The Degree Centralization index indicates the existence of nodes (organizations) very central in the network. Such nodes, if removed, would lead to the dispersion of the others. The calculation of Degree Centralization was applied to the authority relations. This index is measured on a scale from 0 to 01. The closer to zero (0.00), the more resilient, or less prone to fragmentation a network is. One important caveat is the fact that being more resilient can also mean being less able to adapt to new strategic challenges.[19] Therefore, the exact meaning of a particular index requires additional qualitative analysis to be established.

The Betweenness Centralization index indicates how evenly the information is distributed on the network. It is also measured on a 0 to 01 scale. The calculation of Betweenness Centralization was applied to the information flow graphs. The closer to zero (0.00), the better the information is distributed. Obviously, due to security reasons, in the case of national intelligence systems a totally equal dissemination of information across the network is not necessarily desirable or possible. On the other hand, the closer to one (1.00) in terms of Betweenness Centralization, the higher the risk that a single node organization can retain all the information, acting as a gatekeeper on the network.

We have calculated each centralization index (Degree and Betweenness) separately. As the two indexes are already expressed on a scale between 0 and 01, it was not necessary to perform the standardization process. In the following sections one finds the preliminary results for the national intelligence systems of Brazil, Russia, India, China, and South Africa.[20]

Brazil

Created in 1999 by Federal Law 9.883, the current Brazilian Intelligence System (SISBIN) has been characterized by organizational continuity and recurring institutional crises.[21] One reason for that is the preference in Brazilian legislation to use broad definitions of intelligence and threats.[22] Although a less than explicit definition of what intelligence is about is quite common in many countries (the United Kingdom, for example); two institutional consequences of this choice in the case of Brazil are the high inclusiveness of the Brazilian intelligence system and the difficulty in defining missions focused on the provision of national security.[23] In total, the Brazilian national intelligence system included 22 supervising and directing organizations (government), 05 collegial bodies (coordination), and 23 intelligence organizations (agencies).[24]

In Brazil, the president has the highest level of formal authority over the system (a Degree Centrality of 22.37). The actor with the second-highest level is

the Ministry of Justice (7.34). In part, this results from the fact that the president directly subordinates all other governmental supervising and directing organizations (government). Since the Brazilian system is very inclusive, many of these organizations do not have intelligence activities as their primary mission. A critical node is the Brazilian Intelligence Agency (ABIN). Designated by law as the intelligence system center, its leadership in SISBIN is hindered by issues related to budget, priority and focus of its primary mission, as well as personnel and administrative authority. Since 2002, ABIN has been placed under the authority of the Institutional Security Cabinet (GSI) of the presidency. As much for its intermediate position in the chain of command between the presidency and ABIN as for its participation in many collegial organizations for coordination (coordination), the GSI accumulates great power in SISBIN.[25] While the Degree Centrality of ABIN is 1.74, the same index in the case of GSI reaches 3.84. To increase sectoral coordination, preserve autonomy, and develop specific doctrines for military intelligence and public security intelligence, new collegial organizations were created in the early 2000s for coordination, such as the Defense Intelligence System (SINDE) and the Subsystem of Public Security Intelligence (SISP). Respectively, the Ministry of Defense (5.24) and the Ministry of Justice (7.34) have a high degree of centrality due to their roles in these subsystems.[26] The Ministry of Finance, in turn, also has a high centrality index (4.89), which indicates a tendency for the institutionalization of a subsystem of financial intelligence in Brazil.

Regarding the control of information flows, ABIN stands out with a Betweenness Centrality of 32.3. Although it has a low Degree Centrality index, this organization has links with most actors that provide links with other actors, having in fact the shortest geodesic path and the most obvious one as shown by information flow. Therefore, ABIN has power in the system not because of the number of organizations it subordinates, but for its role in the information flow. Given the density of the network, ABIN cannot position itself as a gatekeeper, i.e., as an actor that may impede the information flow.[27]

In sum, power is highly concentrated in the Brazilian National Intelligence System, even if the system itself is not very powerful due to its excessive inclusiveness and lack of effective external control. Only a few actors hold the majority of power resources (authority and information), among them the president, ABIN, and the Ministers of Institutional Security, Finance and to a lesser extent, Justice, and Defense.

Russia

Since the end of the USSR, the structure of the Russian national intelligence system has oscillated in accordance with changes in state capacity, threats to na-

tional interests, and the availability of resources. Since Vladimir Putin's presidential election in 2000, the legacy of Boris Yeltsin has been reverted. Instead of fragmentation and weakening of the intelligence services came a period of increasing power and more resources, especially following the Second War in Chechnya (1999-2009). There was a reduction in the number of intelligence organizations, replacement of several directors, and expansion of operational capabilities, missions and technology base.[28] More recently, despite the crisis in Ukraine and increased tension with the European Union and the United States, the expansion of the Russian intelligence system was put in check by the economic crisis. The legal basis for the functioning of the Russian intelligence system is a set of laws passed in February 2006 (On Counteraction of Terrorism; On Operational Search Activity; On Security), which applies to all the country's intelligence organizations. They complement specific laws called 'On the Federal Security Service' (May 1995) and 'On External Intelligence' (December 1995). There are other laws, decrees and presidential directives. According to Soldatov, major reforms in the Russian secret services did not occur because of September 11, but because of the attack of insurgents in Ingushetia in June 2004.[29] In total, the adjacency matrix (and the resulting graph) of Russia's national intelligence system included 06 governmental supervising organizations (government), no collegial bodies (coordination) and 07 proper intelligence organizations (agencies).

In the case of authority relations within the Russian intelligence system, the president has the highest Degree Centrality (36.84). After the 2006 reforms, the president concentrated even more authority, directly subordinating most organizations in the Russian network. Despite the Federal Security Service (FSB) being considered a central actor, its Degree Centrality index of 3.95 is lower than the Federal Service for Technical and Export Control (FCTEK) (5.26) and equal to organizations such as the Foreign Intelligence Service (SVR), Military Intelligence Directorate (GRU), Federal Protective Service (FSO), Directorate for Military Topography (VTU), or even the Ministry of Internal Affairs (MVD) and the prime minister. Besides the president, the Chief of Staff of the Armed Forces (13.16) and the Ministry of Defense (9.21) have high centrality in the Russian system.

When it comes to information flows, the GRU has the highest Betweenness Centrality (30.91) in the Russian system, higher even than the FSB (22.55). Part of the explanation lies in the fact that many information flows that pass through the FSB are informal, with intensity 03 only. In contrast, the information flows through the GRU are more formal and, therefore, more intense. Besides them, the FCTEK also has a relatively high Betweenness Centrality index (16.48). This can be explained by its role in information security and signals counterintelligence.

This type of mission compels the FCTEK to maintain communication (data streams) with different actors of type 01 (government) and some important organizations of type 03 (agencies). Finally, the Betweenness Centrality index of the president (14.67) is explained by the fact that he directly subordinates all political authorities and all agencies, except GRU and VTU, causing the president's office to be a natural intermediator in many relationships.

The power distribution in the Russian national intelligence system is heavily concentrated in the president. Note that type 02 organizations (coordination) were not included in the Russian system, given the difficulties in obtaining information about the possible role of the National Security Council in relation to the intelligence organizations (agencies).[30] In addition, it is worth noting that most agencies in the system are directly subordinated to the president. The only two agencies that are not directly subordinated are the GRU and the VTU, responsible for imagery intelligence (IMINT). Both organizations are directly subordinated to the Chief of Staff (CGS) which, although being subordinated to the Ministry of Defense, is appointed by the president.

Finally, a word about the centrality of the FSB, the organization responsible for counterintelligence, counterterrorism, and protection of the constitution. Vladimir Putin was FSB director from 1998 to 1999. During most of his tenure as president, the FSB has strengthened and acquired more power. FSB officers have assumed key positions in the MDV and also went on to develop intelligence activities in the fields of SVR and GRU, even taking responsibility for border control.[31] However, in the context of the Ukrainian crisis the Russian President may promote reform in order to reduce the FSB's centrality in the Russian intelligence system.

India

The Indian national intelligence system is strongly guided by regional security challenges, but also by Delhi's objective to become a great power.[32] The broad range of organizations in the system stems from three main factors, namely, the combination of internal security threats (insurgency and communal violence), border conflicts (especially with Pakistan), and regional and global ambitions (positioning towards China and the United States). So far, India has neither specific legislation regulating the operations and activities of its diversified intelligence organizations, nor significant external control mechanisms or congressional oversight. Therefore, defining the size of the intelligence system and its internal relationships becomes a challenge in itself.[33] Fortunately, since intelligence agencies in India are active players in the internal political process of the country, there is considerable debate in the media about their role.[34] The latest reform of the sys-

tem dates from 2002, when the Kargil Committee Report recommended changes that were partially implemented by 2008.[35] In total, the adjacency matrix (and the resulting graph) of India's national intelligence system included 07 governmental supervising and directing organizations (government), 02 collegial organizations (coordination) and 20 intelligence organizations (agencies).

From the authority relations point of view, it is important to highlight in the Indian case the Degree Centrality index of the prime minister (14.29). This can be explained by the PM's close working relationship to other supervising organizations (government), such as the Ministry of Defense (12.50) and the Ministry of Finance (12.50). India has intelligence agencies subordinated to the Ministry of Finance, of which the most important is the Central Economic Intelligence Bureau (CEIB).[36] Similarly, the Degree Centrality of the Defense Ministry is elevated because it subordinates a number of agencies that form a military intelligence cluster. The Ministry of Interior (Home Affairs) has a Degree Centrality index of 5.3, while the Intelligence Bureau's index is 4.76. We would expect the index of the Ministry of Interior to be significantly higher than that of the Intelligence Bureau (IB). However, the actual results reflect the double subordination of the agency to the minister and the prime minister, elevating the Centrality in-degree of the IB. The most important Indian collegial body (coordination) should be the Joint Intelligence Committee (JIC). It is subordinated to the National Security Council (4.79) and consists of the directors of Research and Analysis Wing (RAW) (3.57), the Intelligence Bureau (IB) (4.76), the Defense Intelligence Agency (DIA) (1.79), the three officers of the military intelligence, a senior representative of the Ministry of Defense, and a senior representative of Ministry of Foreign Affairs. However, the JIC has a relatively low Degree Centrality index (1.79). This may indicate that the JIC has not been able to produce effective coordination, mainly because of its reduced staff and infrequent meetings.[37]

Due to the system's size, Betweenness Centrality of the Indian network is concentrated among the system's clusters. The highest indexes are from the National Counter Terrorism Centre (NCTC), which reaches 20.50 for communicating closely with the other agencies on the specific issue of combating terrorism. Also notable are the JIC, with a 13.71 index and, again, the cluster of economic and fiscal intelligence, with Betweenness Centralities of 13.71 (CEIB) and 9.78 (Ministry of Finance), both higher than that of the prime minister (8.21). Betweenness Centralities of the intelligence agencies (organizations of type 03), are relatively low, but significant in the case of defense cluster agencies, RAW (4.68), DIA (3.87), JCB (3.87), and National Technical Research Organization (NTRO) (3.87).

Taken together, the distribution of authority and information flows in India's system indicate that power is firmly in the hands of government supervising organizations (government), with a limited role played by coordinating organizations (type 02). Also, well-defined clusters of power also exist in the area of defense, counter-terrorism, and finance. The financial intelligence cluster demands additional research, but its power seems to be significant in India. The four major intelligence agencies of the Indian system are the IB, RAW, the NTRO, and the DIA. The Intelligence Bureau (IB), which is subordinated to the National Counter Terrorism Center (NCTC), is the agency dedicated to coping with internal security threats and also the main result of the post-Mumbai reform. The RAW is the foreign intelligence agency and its real importance for the state power in India seems to contrast with its relatively low indexes in terms of authority and information control. Both the IB and the RAW are subordinated to the prime minister. As they are frequently reported as having considerable autonomy, such discrepancies between informal accounts and formal institutional arrangements need to be reconciled through additional research. Finally, the two most-important military intelligence agencies are the NTRO, dedicated to technical means of collection, and the DIA, which emulates the U.S. model of consolidating the contributions of the three armed forces.

China

China's national intelligence system defies classification, mainly because of its complexity and incommensurability in relation to the United States of America, the United Kingdom, or even to the other BRICS countries. However, a first step should be to avoid including all state and communist party organs as "potential intelligence organizations."[38] This is not to neglect the central role played by the Communist Party of China (CPC) in the political system as well as in Chinese society. Neither to ignore that as a great power (similar to the United States and Russia), China probably has a very large intelligence system, one with specialized organizations focused on internal, regional, and global security issues. The deep historical continuity of the state in China, its cultural characteristics, or even the Soviet influence in the twentieth century should not obscure the fact that modern military tasks, police, foreign policy, development, and others demanding support from the intelligence system in China are the same found in other countries. This modern national intelligence system emerged along with the military modernization since the 1980s.[39] In total, our account of China's national intelligence system included 10 governmental supervising organizations (government), no collegial body (coordination) and 24 intelligence (agencies).[40]

Constitutionally, the role of the President of the Republic, Chairman of the Central Military Commission (CMC) and the Communist Party of China Secretary General (CPCSG) need not necessarily be held by the same person. That these roles are now held by one person represents a 'de facto' political and institutional arrangement. Given the authority relations with different network nodes, the Degree Centrality index of the president (7.41) is higher than that of the CPCGS (5.09). In addition, both have lower indexes than the CMC (11.11), and an even lower index than that of the Ministry of State Security (MSS) (18.52). This is partially a consequence of the authors' decision to consider the major departments of the MSS separately. Other important ministries are the Ministry of Industry and Information Technology (MIIT) (4.63), the Ministry of Foreign Affairs (MOFA) (3.24) and the Ministry of Public Security (MPS) (2.78). As in the Russian case, type 02 organizations (coordination) were not identified. Given the high functional specialization in the network (division of labor between the nodes) and the large number of agencies, Degree Centralities indexes remain low for all type 03 organizations (agencies), ranging between 1.39 and 2.78.

Although it is very difficult to estimate the flow of information in Chinese intelligence, organizational system configuration indicates that most likely some organizations establish different degrees of communication with others. The especially high values for the Betweenness Centrality index of the Ministry of State Security (36.62) and CPC General Secretary (27.19) stand out as examples. All other nodes in the network show a variation in their Betweenness Centrality indexes ranging from 0 to 5.89, including the president (2.19) and the Central Military Commission (2.86).

Considering the performance of both indexes and similar to what is found in other countries, three actors (nodes) concentrate a lot of power in China's national intelligence system; namely, the MSS and, to a lesser extent, the president and the CMC. In the case of the CMC, the chain of command in the military intelligence cluster encompass the general departments (General Political Department [GPD]; General Staff Department [GSD]; 2nd Department [GSD2]; and 3rd Department [GSD3]), and also the intelligence capabilities of the four singular forces in the People Liberation Army (PLA), namely the PLA ground forces, the PLA Navy, the PLA Air Force, and the PLA Second Artillery Force. Notably, the intelligence capabilities of the People's Armed Police (PAP), the main constabulary force in the country, are subordinated to both the MPS and the CMC. In turn, the MSS and its various departments (bureaus) correspond to an important cluster in Chinese civil intelligence. Finally, unlike other countries where a financial or tax intelligence cluster seems to be taking institutional form, in China what stands out is the growing importance of the GSCPC and MIIT.

South Africa

After the defeat of the apartheid regime, South Africa's national intelligence system underwent two major reorganizations. In 1996, the new constitution established two basic principles for the democratic functioning of South African intelligence: coordination between agencies and civil control of their activities. In the mid-1990s, the Intelligence Law and the White Paper on Intelligence specified the division of intelligence missions in separate agencies (internal and external), with emphasis on external control mechanisms, coordination, supervision, and use of technical means of collection. In 2005, complaints related to illegal operations to intercept communications of ANC (the ruling party) members damaged the legitimacy of the intelligence services and their oversight bodies.[41] In 2009, the new president Jacob Zuma announced changes in the intelligence system, which by 2013 were guided by the General Intelligence Laws Amendment Act. The new structures were designed to produce administrative consolidation, reduce the number of agencies, and to refocus on missions strictly related to national security.[42] In total, the adjacency matrix (and the resulting graph) of South Africa's national intelligence system included 05 supervising organizations (government), 02 collegial bodies (coordination) and 11 intelligence organizations (agencies).

In terms of authority, the South African President's Degree Centrality index (18) is lower than that of the State Security Agency (SSA) (20). Although the president subordinates all ministries and is not subordinate to any other node in the network, making his out-degree higher than that of the SSA, the Total Degree is lower because the composite index considers all subordinative relations in which an actor is involved. As the SSA answers to the president and the Ministry of State Security, but subordinates the six branches that comprise it since the 2009 reform, its Degree Centrality is higher. All other organizations in South Africa's Intelligence System have Degree Centrality indexes ranging between 02 and 07.

The president has the largest Betweenness Degree in the South African case (38.85). This indicates that all three types of organizations communicate with each other through the presidency. The Betweenness Centrality index is also high for the National Intelligence Coordinating Committee (22.29) and the Financial Intelligence Centre (18.17). Although the National Intelligence Coordinating Committee's (NICOC) case is relevant to support the intention of transforming the committee into a major locus of communication between network nodes, the case of Financial Intelligence Centre (FIC) stands out as a result of the large number of informal relationships with other organizations in the intelligence sys-

tem. As observed in other countries, the so-called financial or tax intelligence cluster has grown in importance and demands further study.

In fact, the power distribution in South Africa's national intelligence system tilts heavily to the president and the SSA. Besides them, we highlight the NICOC and the FIC. The importance of the SSA cannot be underestimated in the current configuration (post-2009) of the South African intelligence system. This agency also concentrates corporate services (human resources, IT, infrastructure, logistics and finance) previously redundant in different agencies. It is also in charge of ensuring unity of command and consistency of objectives for the different branches of the intelligence activity: the internal, the external, and the technical. Because of the SSA's position in the network, the president does not directly subordinate any intelligence agency.

Finally, a summary of the results obtained in the five countries can be seen in Table 01.

Country	Unit Types			Unit Indexes				Network Indexes	
	GOV	COO	AGE	Highest Degree Centralities		Highest Betweenness Centralities		Degree Centralization	Betweenness Centralization
				Unit	Value	Unit	Value		
BR	22	05	23	PR	22.38	ABIN	32.38	0.206	0.314
RU	06	0	07	PR	36.84	GRU	30.91	0.364	0.208
IN	07	02	20	PM	14.29	NCTC	20.50	0.116	0.260
CH	10	0	24	MSS	18.52	GSCPC	27.19	0.184	0.428
SA	05	02	11	SSA	20	PR	38.85	0.159	0.394

Table 1: National intelligence systems in the BRICS group

Conclusions

In this article, we have tried to answer three questions: 01. How are the national intelligence systems organized in the BRICS countries? 02. How is power distributed among specific organizations in each national intelligence system? 03. What are the implications of a given distribution of power to the system's overall organizational risk?

Regarding the first question, a few commonalities and various specificities were observed in the cases of Brazil, Russia, India, China, and South Africa. For example, Russia and India have civilian intelligence agencies specialized in collecting and analyzing intelligence about international security threats. In the cases of China (MSS) and South Africa (SSA), the same missions and functions are performed by specialized branches (bureaus) of larger organizations. Brazil is the

only country in this sample with no major civilian intelligence agency primarily focused on external threats. Even so, the overall number of organizations involved in each national intelligence system is much higher in Brazil (50), China (34), and India (29) than in South Africa (18) and Russia (13).

This alone cannot be taken as an indicator of how capable or efficient a given intelligence system is. For instance, Russia is a great nuclear power with advanced conventional weaponry and significant force projection capabilities, but has only 07 main intelligence agencies. On the other hand, Brazil is a regional power with 23 main intelligence agencies. In the case of China and South Africa, we stand by our decision to consider specialized branches of MSS and SSA as distinct agencies for analytical purposes. Even so, India (20) and China (24) have similar numbers of intelligence agencies despite their different political regimes. One organizational feature that seems to be associated with a polyarchic form of government is the presence of collegiate bodies to coordinate different parts of the national intelligence systems. Institutions like South Africa's NICOC, India's JIC, and Brazil's SISBIN Council have no equivalents in Russia or China.

As for the second question, by employing node (organization) level measures of Degree Centrality (authority) and Betweenness Centrality (information) we were able to assess how power distribution varies in the five national intelligence systems. As predicted by theories of intelligence systems evolution, rulers (democratic and otherwise) create agencies to expand the surveillance and awareness capabilities of the state.[43] However, they are probably aware that creating multiple agencies helps prevent one agency from becoming too powerful and usurping the ruler.[44] Therefore, one should expect government principals to enjoy more power than intelligence agencies.[45] Whatever the political regime type (presidential, parliamentary, or communist), well-established states are characterized by intelligence subordination to the political authorities. Presidents have the highest Degree Centralities (authority) in Russia (36.84) and Brazil (22.38), as does the prime minister in India (14.29). In the cases of China and South Africa, the highest Degree Centralities are respectively those of the MSS (18.52) and the SSA (20).

This is not to say that intelligence agencies are powerless. Their power comes from their control of important information flows (Betweenness Centrality). Besides, much of an intelligence agency's power comes from its attachment to a powerful cabinet-level sponsor. We found this feature in the case of ABIN in Brazil, FSB in Russia, IB and RAW in India, or the various intelligence bureaus of the Ministry of State Security in China. Even the now-powerful State Security Agency in South Africa is subordinated to a Ministry of State Security (the successor of the Ministry of Intelligence Services). Whenever an agency seeks to concentrate too much power, the political authority starts mobilizing to avoid it,

as we observed in the case of Russia's FSB. The highest Betweenness Centrality degrees observed in the five countries were those of ABIN in Brazil (32.38), GRU in Russia (30.91), and NCTC in India (20.50). In contrast, in China and South Africa the highest Betweenness Centralities are those of the General Secretary of the CPC (27.19) and the president (38.85), respectively.

Finally, we have also tried to compare the cases at graph level with respect to the organizational risk posed by a particular distribution of power. As a reminder, organizational risk is the probability that internal vulnerabilities or external threats will adversely affect the network. We use Degree Centralization to measure resilience/adaptability and Betweenness Centralization to measure information concentration. The respective Centralization indexes for Brazil (0.206), Russia (0.364), India (0.116), China (0.184), and South Africa (0.159) indicate that Russia runs the highest risk of having an intelligence system less able to adapt to changing strategic circumstances, at the same time being the most resilient among the five countries.

Unfortunately, one cannot say from this index how President Putin's reform efforts will impact Russian intelligence, or if the Ukrainian crisis will force any kind of institutional stress. Likewise, the respective Betweenness Centralization indexes for Brazil (0.314), Russia (0.208), India (0.26), China (0.428), and South Africa (0.394) indicate that China has the highest risk of a single actor (MSS) being able to retain most of the information, acting as a gatekeeper on the network. Of course, the index itself reveals nothing about actual tendencies or evidence of what the CMC, the president or the MSS intend to do. However, the current crackdown on corruption under Xi Jinping's rule bears watching from a Network Analysis standpoint.

Network Analysis has proved to be a useful approach to promote a comparative research program in the Intelligence Studies field. So far, we were able to offer a systematic way of describing national intelligence systems in such relevant countries as Brazil, Russia, India, China, and South Africa. It was also possible to state with some corroboration the existence of a causal relationship between certain organizational settings and a higher or lower level of organizational risk in the case of national intelligence systems. Aware of the Network Analysis limitations, researchers will continue to explore its potential. For example, by integrating more data on external control organizations in the legislative and judiciary branches of government. With new measurements and updated data, even better interpretations of results shall follow.

Notes

1. Peter Gill and Mark Phythian, "What is intelligence studies?" *The International Journal of Intelligence, Security, and Public Affairs* 18, no. 1 (2016): 10; Mark M. Lowenthal, *Intelligence: from secrets to policy*, Sixth edition (Thousand Oaks, California: CQ Press, 2015), 37-69.

2. Wilhelm Agrell and Gregory F. Treverton, ed., *National intelligence systems: current research and future prospects* (Cambridge: Cambridge University, 2009), 304; Steven Boraz and Thomas Bruneau, ed. *Reforming intelligence: obstacles to democratic control and effectiveness* (Austin: University of Texas Press, 2007), 407; Philip H. J Davies and Kristian C. Gustafson, ed., *Intelligence elsewhere: spies and espionage outside the Anglosphere* (Washington: Georgetown University Press, 2013), 256; Peter Gill, "Evaluating intelligence oversight committees: the UK intelligence and security committee and the 'war on terror,'" *Intelligence and National Security* 22, no. 1 (2007): 14-37; Glenn Hastedt, "Towards the comparative study of intelligence," *Conflict Quarterly* 11 (1991): 55-72; Michael Herman, *Intelligence power in peace and war* (Cambridge: Cambridge University Press, 1996), 438; Kevin M. O'Connell, "Thinking about intelligence comparatively," *Brown Journal of World Affairs* 11, no. 1 (2004): 189-199.

3. Michael M. Andregg and Peter Gill, "Comparing the democratization of intelligence," *Intelligence and National Security* 29, no. 4 (2014): 487-497; Hans Born and Ian Leigh, "Democratic accountability of intelligence services," policy paper (Geneva: Geneva Centre for the Democratic Control of Armed Forces (DCAF), 2007); Stuart Farson; Peter Gill; Mark Phythian and Shlomo Shpiro, eds., *PSI handbook of global security and intelligence: national approaches*, two volumes (Westport/London: Praeger Publishers, 2008), 700; Susana C. Lemozy and Russell G. Swenson, eds., *Democratization of intelligence: melding strategic intelligence and national discourse* (Washington, DC: National Defense Intelligence College, 2003), 127; José Manuel Ugarte, *Legislación de inteligencia* (Buenos Aires: Editorial Dunken, 2001), 518.

4. Marco Cepik and Christiano Ambros, "Intelligence, crisis and democracy: institutional punctuations in Brazil, Colombia, South Africa and India," *Intelligence and National Security* 29, no. 4 (2014): 523-551; Eduardo E. Estévez, "Comparing intelligence democratization in Latin America: Argentina, Peru and Ecuador cases," *Intelligence and National Security* 29, no. 4 (2014): 552-580; Mark Phythian, "Intelligence theory and theories of international relations: shared world or separate world?" in *Intelligence theory: key questions and debates*, ed. Peter Gill, Stephen Marrin, and Mark Phythian (New York: Routledge, 2008), 54-72.

5. For discussion of the meaning and the various ways to classify the BRICS countries, see Andre Cooper and Daniel Flemes, "Foreign policy strategies of emerging powers in a multipolar world: an introductory review," *Third World Quarterly* 34, no. 8 (2013): 943-962; Andrew Hurrell, "Rising powers and the emerging global order," in *The globalization of world politics: an introduction to international relations*, ed. John Baylis, Steve Smith, and Patricia Owens (Oxford: Oxford University Press, 2014), 80-94; and Paulo Fagundes Visentini, Gabriel Adam, Maíra Vieira, André Silva, and Analúcia Pereira, *BRICS: as potências emergentes: China, Russia, Índia, Brasil e África do Sul* (Rio de Janeiro: Editora Vozes, 2013), 232.

6. Helen Armstrong, Anthony Johnson, and Ian Mcculloh, *Social network analysis with applications* (New Jersey: John Wiley & Sons, 2013), 18.

7. According to the hypothesis proposed by Cepik and Ambros, one of the variables that affect the learning capacity and the evolution of national intelligence systems is the degree of functional differentiation (division of labor) observed in each country.

8. Robert A. Hanneman and Mark Riddle, *Introduction to social network methods* (Riverside: University of California Press, 2005), 60.

9. The specific sources for each country are referred to throughout the article.

10. Andregg and Gill, "Comparing the democratization of intelligence," 488.

11. Patrick R. Keefe, "Privatized spying: the emerging intelligence industry," in *The Oxford handbook of national security intelligence*, ed. Loch K. Johnson (Oxford: Oxford University Press, 2010), 296-309.

12. Graphs (G) are abstract objects formed by a set V of vertices (or nodes) and a set E of edges (or links). That is, G = (V, E). Graph theory and relational algebra are the mathematical basis of the Network Analysis

area. Other important methodological foundations are the Statistics and Computational Algorithms; Ulrik Brandes and Thomas Elerbach, eds., *Network analysis*: *methodological foundations* (Berlin: Springer, 2005), 472.

13. Cf. http://www.casos.cs.cmu.edu/projects/ora/software.php. Other network analysis software do exist. See Mark Huisman and Marijtje A. J. Van Duijn, "A reader's guide to social network analysis software," in *The SAGE handbook of social network analysis*, ed. John Scott and Peter J. Carrington (Washington: SAGE Publications Ltd, 2011), 578-597.

14. Brandes and Erlebach, *Network analysis*, 92-95; Further discussion about the insufficiency of centrality indexes to measure power to be found in Stephen P. Borgatti, "Centrality and network flow," *Social Networks* 27 (2005): 55–71.

15. Linton C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks* 1 (1979): 215-239.

16. Armstrong, Johnson, and Mcculloh, *Social network analysis with applications*, 320; Hanneman and Riddle, *Introduction to social network methods*.

17. Armstrong, Johnson, and Mcculloh, *Social network analysis with applications*, 205-234.

18. According to Cepik and Ambros, organizational risk in this sense is conducive to institutional crises, which tends to be more recurrent in the intelligence realm than in other areas of government due to secrecy, lack of proper external controls, as well as low functional differentiation.

19. As Russell Swenson called to our attention (e-mail to the authors), "greater resiliency, in more cultural terms, could also imply that no hegemon exists among members of the system that would insist on other organizations becoming adaptive to new situations or threats. That is, each bureaucratic unit is able to maintain its old habits, even if less productive than before."

20. Besides, two types of annexes can be found as online supplements on the Brazilian Political Science Review website. First, tables for each country detailing the names of all organizations, their types (government, coordination, agency) and the values of both indexes (Degree and Betweenness). Second, graphs (one for each country) where the nodes colored in red are type 01 organizations (government), the nodes colored in green type 02 organizations (coordination), while the blue ones are type 03 organizations (agencies). Although it is not possible to visualize each link individually, the darker the color of the edge the more intense is the relationship of authority or communication.

21. Priscila C. Brandão, *Serviços secretos e democracia no Cone Sul: premissas para uma convivência legítima, eficiente e profissional* (Niterói: Impetus, 2010), 302; Marco Cepik, "Regime político e sistema de inteligência no Brasil: legitimidade e efetividade como desafios institucionais," *DADOS* 48, no. 1 (2005): 67-113; Marco Cepik, "Structural change and democratic control of intelligence in Brazil," in *Reforming intelligence: obstacles to democratic control and effectiveness*, ed. Thomas Bruneau and Steven Boraz (Austin: University of Texas Press, 2007): 149-169; Joanisval Brito Goncalves, "The spies who came from the tropics: intelligence services and democracy in Brazil," *Intelligence and National Security* 29, no. 4 (2014): 581–599.

22. Marco Cepik, *Espionagem e democracia* (Rio de Janeiro: Editora, 2003), 207-212.

23. In addition to the Law 9,883/1999, the organization and the functioning of SISBIN are regulated by Decree 4,376/2002. The Decree 8,793/2016 establishing the first ever public guidelines for a National Intelligence Policy was finally issued (after more than five years of expectations) by the interim Temer government in June 2016, in the midst of controversial impeachment procedures against the President elected Dilma Rousseff. Reflecting the need of legal and legitimacy reassurances in times of vicious political turmoil, the new National Intelligence Policy limits itself to reiterate the strict adherence of Brazilian intelligence activities to the Constitutional principles. Of much more positive consequence—if it ever overcomes the National Congress maze—is the Law Project (Bill) 3,578/2015, introduced by Representative Jô Moraes (PCdoB/MG) to regulate ABIN's operational procedures and judicial control of secret intelligence collection in the country.

24. The Public Prosecutor's Office (MP) is the Brazilian body of independent public prosecutors at both the federal (Ministério Público da União) and state level (Ministério Público Estadual). The intelligence roles played by specific organizations inside the MP seems to be increasing, but they were not included this time because they are not an official part of SISBIN.

25. The Director of ABIN is a civilian who has to go through confirmation hearings of his name in the Senate, while the Minister of the Institutional Security Office (GSI) has been an officer of the Armed Forces appointed by the President of Republic. This arrangement is problematic for the democratic functioning of the intelligence in Brazil; Luiz Carlos de Carvalho Roth, "Uti exploratoribus: credibilidade e controle da atividade de inteligência no Brasil," Masters dissertation, Ciência Política (Niterói: Universidade Federal Fluminense, 2009).

26. Originally, ABIN exercised the SISP coordination function. One of the reasons for the transfer of responsibility to SENASP was the existence of operational problems and disputes between ABIN and Ministry of Justice. Still, the SENASP itself finds resistance from the Federal Police, which, in turn, also presents difficulties in cooperation with other state police; Marco Cepik, "Regime político e sistema de inteligência no Brasil: legitimidade e efetividade como desafios institucionais," *DADOS* 48, no. 1 (2005): 67-113.

27. A finding that reinforces recent studies on the development of intelligence systems in Brazil is the high Betweeness Centrality (7.3) of the Operations and Management Center of the Amazonian Protection System (CENSIPAM). Created in 2002 with a focus on a critical region for the security and the development of Brazil, the Center provides joint experience for actors from different parts of the system and focuses on results, stimulating inter-agency cooperation. See Flávio César de Siqueira Marques, "Fusão de dados na inteligência militar," Doctoral thesis, Ciências Militares (Rio de Janeiro: Escola de Comando e Estado Maior do Exército (ECEME), 2016); and Túlio Marcos Santos Cerávolo, "A integração da inteligência nas operações interagências no Brasil contemporâneo," Masters dissertation, Ciências Militares (Rio de Janeiro: Escola de Comando e Estado Maior do Exército (ECEME), 2014).

28. Mark Galeotti and Johnny Shumate, *Russian security and paramilitary forces since 1991* (Oxford: Osprey Publishing, 2013), 64; Andrei Soldatov, "Russia," in *PSI handbook of global security and intelligence: national approaches*, ed. Stuart Farson, Peter Gill, Mark Phythian, and Shlomo Shpiro (Westport/London: Praeger Publishers, 2008), 479-497.

29. Soldatov, "Russia."

30. See also the National Antiterrorist Committee (NAK), established in 2006. It is subordinated to the FSB, but we could not assess if it has authority over other intelligence agencies. Within the Commonwealth of Independent States (CIS) there is a Commonwealth of Independent States Anti-Terrorism Center (CIS ATC), established in 2000 to coordinate the exchange of information among member countries of the institution, http://www.iacis.ru/eng/about/partners/partnerskie_organizatsii/antiterroristicheskiy_tsentr_sng.

31. Galeotti and Shumate, *Russian security and paramilitary forces since 1991*.

32. Marco Cepik, "Segurança nacional e cooperação Sul-Sul: Índia, África do Sul e Brasil," in *Brasil, Índia e África do Sul: desafios e oportunidades para novas parcerias*, ed., Maria Regina Soares de Lima and Monica Hirst (São Paulo: Paz e Terra, 2009), 63-118.

33. N. C. Ashtana and Anajali Nirmal, *Intelligence and security management* (Jaipur: Pointer Publishers, 2004), 454.

34. Rana Banerij, "Legalising intelligence gathering," *The Hindu* 8 July 2014, http://www.thehindu.com/opinion/op-ed/legalising-intelligence-gathering/article6186885.ece?css=print.

35. Created after attacks on Pakistani Kargil district of Ladakh region in 1999 and discussed the course of Indo-Pakistani relations since 1947, the proxy war in Kashmir, and the nuclear issue. The committee sought to determine whether the type of aggression occurred could have been anticipated by the intelligence services and what were the possible failures that allowed the surprise attack. Many of the proposals, however, were only implemented in 2008, after the attacks in Mumbai, whose authorship is still debated; Cepik and Ambros, "Intelligence, crisis and democracy."

36. Bruce Vaughn, "The use and abuse of intelligence services in India," *Intelligence and National Security* 08, no. 1 (1993): 01-22.

37. Major General V. K. Singh, *India's external intelligence: secrets of research and analysis wing (RAW)* (New Delhi: Manas Publications, 2007), 157-170; Vaughn, "The use and abuse of intelligence services in India."

38. This is a common error incurred by ideologically motivated observers. One example is the otherwise useful volume by the French journalist Roger Faligot, *O serviço secreto chinês* (São Paulo: Larousse, 2009), 543.

39. For the general security context see chapter 18 of Henry Kissinger, *On China* (New York: Penguin Press, 2011), 624; as well as David Shambaugh, *China goes global: the partial power* (Oxford: Oxford University Press, 2013), 432. Regarding the intelligence component of the military modernization in China, see Dennis J. Blasko, *The Chinese army today: tradition and transformation for the 21st Century* (New York: Routledge, 2006), 256; as well as Anthony H. Cordesman and Martin Kleiber, *Chinese military modernization: force development and strategic capabilities* (Washington: CSIS, 2007), 226.

40. After taking into consideration their specific missions, technical requirements, organizational dimensions, and amount of people employed, we came to the analytical decision of considering 12 specific bureaux under the authority of the Ministry of State Security (MSS) as distinct intelligence agencies. Otherwise the total number of intelligence agencies in China would be reduced to 12 down from 24. See Xuezhi Guo, *China's security state: philosophy, evolution, politics* (Cambridge: Cambridge University Press, 2012), 496.

41. The Project Avani was an intelligence operation designed to assess the impact of the presidential Succession battle of ANC on the country's stability. As part of this project, the NIA intercepted e-mails from people in senior positions, who allegedly conspired to block the possibility of Zuma becoming the president of the ANC. The inspector general concluded that the emails were false and recommended disciplinary action against those responsible. The director of the NIA at the time (Masetlha) was dismissed by President Mbeki, as well as two senior officers; Kevin O'Brien, "Controlling the hydra: a historical analysis of South African intelligence accountability," in *Who's watching the spies? Establishing intelligence service accountability*, ed. Hans Born (Geneva: Geneva Centre for the Democratic Control of Armed Forces (DCAF), 2005), 199-222.

42. Cepik and Ambros, "Intelligence, crisis and democracy," 541-545.

43. David H. Bayley, "The police and political development in Europe," in *The formation of national states in Western Europe*, ed. Charles Tilly (Princeton: Princeton University Press, 1975), 328-379; Cepik, *Espionagem e democracia*; Charles Tilly, *Coerção, capital e estados europeus: 1990-1992* (São Paulo: EdUSP, 1996), 356.

44. Russell Swenson has called our attention (e-mail to the authors) to this particular important motivation for rulers to design Intelligence Systems with more than one agency. See Peter Gill, *Policing politics: security intelligence and the liberal democratic state* (New York: Routledge, 1994), 384; and also Florina Cristiana Matei, and Thomas Bruneau, "Intelligence reform in new democracies: factors supporting or arresting progress," *Democratization* 18, no. 3 (2011): 602 –630. For historical examples when an intelligence and security apparatus became too powerful up to a point of usurping power to itself by forming a police state (Brazil's SNI or South Africa's BOSS).

45. For an institutionalist theory of intelligence systems development, see Amy B. Zegart, *Flawed by design: the evolution of the CIA, JCS, and NSC* (Stanford: Stanford University Press, 1999), 336. Power-based and institutionalist approaches toward national security are not mutually exclusive.