UNIVERSITATEA „BABEȘ-BOLYAI”

CLUJ-NAPOCA

FACULTATEA DE ȘTIINȚE POLITICE, ADMINISTRATIVE ȘI ALE COMUNICĂRII

ȘCOALA DOCTORALĂ DE ȘTIINȚE POLITICE ȘI ALE COMUNICĂRII

The Play of Hacking and the Political Values of the Hacker Culture

SUMMARY
in English

Conducător de doctorat:
Prof. univ. dr. Vasile Boari

Student-doctorand:
Vlad Bogdan Jecan

Keywords: play, strategic culture, hacktivism, hacking, cyberspace

In a few months, the 24th annual hacker meeting will take place in Paris. The first time hacker met openly was in 1993 at DEFCON, during a period of time when they were perceived as criminals. So, then, how come if hacking is illegal a public meeting of criminals in which they publicly show criminal tricks can take place? Even if hackers have been described as trespassers and thieves, investigated and arrested by the FBI, they have multiple conferences where they present their own specific ways of understanding computer technologies. Famous figures such as Bill Gates, Steve Jobs, Steve Wozniak, and others less known as Linus Torvalds or Sir Tim Berners-Lee have been involved with hacking at one point.

Hackers are being portrayed ambivalently. Big screen productions show hackers as teenagers playing with computers and sometimes have unintended consequences. The cyberpunk literary movement proposed the positive and negative aspects of cyberspace, artificial intelligence, and the technological future, where hacking has the potential to create and stand against various manifestations of power (political, social, technological, military, etc.). Hacking, then, reveals itself to have the potential to offer knowledge and information, destruction and dread. Hacking as a process is usually presented as an unorthodox way of breaking security rules and conventions. It is sometimes nonserious, but serious for the hacker. It reveals itself to be a sort of game. Hacking has become political in recent years. Hacktivism, the term coined to describe political hacking, emerges as a new field of study. In our view, to comprehend the complexity of hacking and the political hacktivism, we cannot rely entirely on a positivist approach. Our research questions, then, are (1) is hacking is a form of play? (2) If so, then, is *hacktivism* is a form of ludic political protest in cyberspace? (3) Can we measure the political preferences of hackers? (4) If so, can we provide the essential political hacker values? Our methodology, therefore, requires theories of the *ludic* from philosophy, sociology, and cultural history, to analyze hacking, while the theory of *strategic culture* from military and security studies coupled with data-driven text analysis reveals the political values of hacktivism and the hacker culture as a whole. The paradigm of play is generous, but it needs to be understood in the parameters explained in Chapter 3. It allows us to see the specific mechanisms through which the hacker culture develops and how it manifests politically. There are, of course, multiple perspectives on hacking, but the ludic approach can reveal the hacker culture. following the formal elements of play defined by Huizinga, for this study we see the play of hacking ending with the process of hacking in cyberspace. Hacking needs to be recognized through the rules that

it proposes (see Chapter 3) and the hacker understands and applies the rules. Individuals who are proficient programmers are not necessarily hackers. We look at different definitions of hacking, from sociological to the definition provided by the Hacker Jargon File. However, we find that the definitions describe hacking rather than explain it. Therefore, for our research we do not focus on a specific definition, but try to understand hacking within the parameters described above.

In the first chapter, titled *Play,* we have set up the methodological parameters to interpret the nature of play and the formal elements of play within hacking. In the nature of play, what we try to identify initially, is the potential positive outcomes that play offers. Therefore, we define the ludic approach through the interpretations of Mihai I. Spariosu of mostly pre-Socratic and Platonic understandings of play. In Archaic Greece, play, according to Mihai I. Spariosu, is initially connected to the notion of immediate physical force. Only sporadically, in the Homeric epics, we find that there are moments in which *agon* and *athlon* are detached from this connotation. In Homer, the play as *agon* is quite evident especially in the counsel that Peleus gives Achilles: "always be best and excel others." The Trojan War offers the opportunity for heroes to seek out moments in which they can show their virtue (*arête*) during a war game (*aristeia)*. During the war game, they become "charmed" (battle-lust) with adrenaline of battle. However, in moments of peace this violent, power-based archaic mentality of might makes right, ceases to exist and peace takes its place. Hesiod and Heralitus appeal to *agon* only to question them directly.

The shift towards a different set of values and interpretation of play is available in Plato. Spariosu notes that *paidia* (children's play) is used as a tool of education. In *Republic*, Socrates detaches play from violence, but returns to it later as education needs to recognize the existence of violence. Following the interpretation of Spariosu, we suggest that the *ludic* has the potential to replace violent and coercive attitudes with that of positive, innovative, and efficient outcomes. A different playground is perhaps needed and cyberspace is an excellent opportunity for such play. The alternative nature of play has been set and now we need to ask the questions necessary to identify acts of play.

In the section of the chapter title *Structural Characteristics of Play*, we discuss Johan Huizinga's work, *Homo Ludens*. Huizinga's interpretation of play, that makes reference to *agon*,

Plato, and the potential positive outcomes, allows us to clearly observe and define moments or processes of play. The Dutch cultural historian offers the following definition of play:

> "Summing up the formal characteristics of play we might call it a free activity standing quite consciously outside "ordinary" life as being "not serious", but at the same time absorbing the player intensely and utterly. It is an activity connected with no material interest, and no profit can be gained by it. It proceeds within its own proper boundaries of time and space according to fixed rules and in an orderly manner. It promotes the formation of social groupings, which tend to surround themselves with secrecy and to stress their difference from the common world by disguise or other means."[1]

The structural characteristics of play are: freedom to engage in the activity, a necessity to replace reality with a new environment where to engage in play; it has a beginning and an end; it creates order and, finally, it has a specific feature of secrecy. Hacking and hacktivism, therefore, in order to be acts of play need to follow these structural characteristics of play. These characteristics are applied to hacking later.

Strategic culture offers us the possibility to establish the sources and metrics for the data-driven analysis of the hacker culture. Our understanding of strategic culture rests on the works of two important scholars on the subject: Jack Snyder and Alastair Iain Johnston. The former starts his analysis on the assumption that Soviet strategic decision makers and American strategic decision makers are not except from their culture. Snyder argues that instead of trying to analyze Russian-Soviet strategic attitudes solely based on game theory, a constructivist approach is capable of adding important contributions to the discussion. Snyder argues that strategic culture, just as culture in general, is not static, but dynamic. It changes according to new influences, but there is always a "residual degree of continuity" from the original values. This concept allows us to identify *trends* in the data visualized on the hacker culture.

According to Snyder, strategic culture can be defined as following:

> "Strategic culture can be defined as the sum total of ideas, conditioned emotional responses, and patterns of habitual behavior that members of a national strategic community have acquired through instruction of imitation and share with each other with

[1] Huizinga, Johan, *Homo Ludens. A Study of the Play-Element in Culture*, The Beacon Press, 1960, p. 13

regard to nuclear strategy."[2]

It is possible, therefore, to find the "sum total of ideas" and other aspects of the hacker culture. However, the definition is quite broad and has been used in studies of a descriptive nature. For the hacker culture, we do not intend to have a similar descriptive approach. While occasionally it is inevitable, we want to address the nature of hacking so we can interpret political hacking in general.

Alastair Iain Johnston in his book, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*,[3] proposes to (1) determine the existence and persistence of strategic culture throughout time and across actors in a given society, on a level that it can be viewed as a "dominant variable" for decision making; and (2) if strategic culture actually influences the behavior of actors. For Johnston, strategic culture is:

> "… an integrated system of symbols (i.e., argumentation structures, languages, analogies, metaphors, etc.,) that acts to establish pervasive and long-lasting grand strategic preferences by formulating concepts of the role and efficacy of military force in interstate political affairs, and by clothing these conceptions with such an aura of factuality that the strategic preferences seem uniquely realistic and efficacious."[4]

It is within cultural artifacts that we can discover "an integrated system of symbols." These cultural artifacts are, according to Johnston, relevant documents that contain the values of a certain culture. Colin S. Gray warns, however, that too much emphasize on strategic culture can imply that it is possible to understand everything and therefore nothing. Gray suggests to view strategic culture in the Latin original meaning, that of *contextere* or "to weave together." In this way, strategic culture is not the causal factor, or the independent variable, that can offer precise prescriptions of future strategic behavior, but the *Geist* that brings the elements of culture (transmitted ideas, attitudes, traditions, and so on) together in order to suggest possible strategic behavior. Colin S. Gray suggests that strategic culture is best viewed as an always-present

[2] Snyder, Jack, *The Soviet Strategic Culture: Implications for Limited Nuclear Operations*, RAND, 1977, p. 9
[3] Johnston, Alastair, Iain, *Cultural Realism: Strategic Culture and Grand Strategy in Chinese History*, Princeton University Press, 1995
[4] *Ibidem*, p. 37

context, as *Geist*, or *being 'out there.'* We subscribe to this idea and use strategic culture for the measurement of the hacker culture. Overall, strategic culture allows us to see not the formation of the culture, for which the ludic approach would suffice, but explore the hacker culture in measurable characteristics.

In the next chapter, *Hacking*, we apply the play and strategic culture to understand the initial stages of political hacking. According to Bernadette Schell and John Dodge there are four phases of "hackerdom history." A *Prehistory*, which starts in the 1800s and ends in 1969, the *Elder Days* from 1970 – 1979, a time that is mostly characterized by phone phreaking, *The Golden Age* from 1980 to 1989 and, finally, *The Great Hacker Wars* and *Hacker Activism* from 1990 to the present.[5] Tim Jordan and Paul A. Tyler distinguish between three categories of hackers. Initially, according to the authors, there were *the original hackers* or the computer scientists who have pioneered the development of networked computing between 1950s and 1960s. In the 1970s, Jordan and Taylor place the *hardware hackers* or hardware innovators who have contributed significantly to the development of the personal computer. Then, there were the *software hackers* who focused mainly on developing computer programs that would be capable to run on different hardware. As the authors note, the three hacking communities often have never been distinct from one another.[6]

The usual distinction between hackers is according to the platform used and intentions. First, we have the oldest form of hacking that is *phreaking* or *phone phreaking* which involves an interest with telephone systems and, later, mobile telephony. *Whitehat hacking* is the law-abiding process of system improvement and innovation. *Greyhat hacking* operates at the limits of lawfulness while sometimes breaking the law on purpose. The end goal is important. The literature points out that greyhat hackers usually perform acts of hacking, that are not always authorized and legal, to draw attention to security weaknesses. *Blackhat hackers* are the malware writers and, in general, individuals who have the skills and knowledge but perform cyber crimes.

In the subchapter titled, *Hacking as Play*, we apply the formal characteristics of play to hacking. The characteristics are the following: : (1) freedom to engage in the activity, (2) a necessity to replace reality with a new environment where to engage in play; (3) it has a

[5] Schell, Bernadette, H., Dodge, John, L., *The Hacking of America*, Quorum Books, 2002
[6] Jordan, Tim, Taylor, Paul, A., *Hacktivism and Cyberwars. Rebels with a cause, Routledge*, 2004

beginning and an end; it (4) creates order and, finally, (5) it has a specific feature of secrecy. In the first case, hackers engage in the activity based on their own free will. There is no political or social coercive action for hacking. We have also looked at the motivations that individuals engaged in the activity have provided. In a series of interviews conducted by Paul A. Taylor,[7] a pattern emerges regarding the choice of hacking. Hackers usually refer to a desire to understand systems and learn how they operate. To discover knowledge about the workings of cyberspace, but also because of a sense of empowerment by feeling better, more skilled, more knowledgeable about a system than the system administrator. The second characteristic allows individuals to replace reality with a new temporary space for the play. Hackers differentiate between the real world and the online, unreal, world. Bruce Sterling writes that for hackers cyberspace isn't real.[8] Svetlana Nikitina compared hackers to trickster gods.[9] The mythical space is, at the same time, the need to replace the actual space. This space is available only for the duration of the game. Therefore, it is implicit that hacking has a beginning and an end. The most interesting of the play characteristics is that it creates order. Through order we understand the rules of the game. In the case of hacking, scholarly literature points to a set of features that the hack requires. If those features are not met, the individual claiming to be hacking is called by the community the derogatory term of *script kiddie*. The features are: simplicity, mastery, illicitness, and original. The hack needs to be a simple solution to a complex problem when the hacker has illicitly acquired enough information about the target system that had developed mastery over it and nobody else managed to do that before. Finally, secrecy is the aspect given by initiation in the hacker culture. That initiation is simple, the individual needs to know and understand the rules of hacking.

The cultural artifacts selected for the study are the Youth International Party Line newsletter, Phrack Magazine and 2600 Magazine. In the case of YIPL, we have conducted our analysis on the first 10 issues. This allows us to identify the source and first ideas of the hacker culture. Phrack Magazine published so-called Hacker Pro-Philes, that are profiles on prominent members of the community. These profiles show hackers view hacking and socio-political issues. 2600 Magazine offers opinion articles on current events and have something similar with

[7] Taylor, Paul, A., *Hackers. Crime in the digital sublime*, Routledge, 1999
[8] Sterling, Bruce, *The Hacker Crackdown*, Bantam Books, 1992
[9] Nikitina, Svetlana, Hackers as Tricksters of the Digital Age: Creativity in Hacker Culture, in *Journal of Popular Culture*, Vol. 45, No. 1, pp. 133 – 152

the Pro-Philes, but in the form of an interview with a famous hacker or individuals familiar with the hacker scene. YIPL was first published in 1971 and had a serious impact on the hacker culture. Scholars note that it may have been this publication that guided the hacker culture onward. Phrack Magazine started in November 17, 1985 and the last issue available for us is from April 14, 2012. 2600 Magazine was first released in 1983 and the last issue was published in Autumn 2015 which gives it a tradition of over 32 years. It became a vehicle for the spread of hacker values that make up the hacker culture. 2600 tends to publish more political perspectives that came to define the hacker culture and have a major influence on hacktivism

Graph generation and interpretation method. The graphs were created using NodeXL, a Microsoft Excel Template developed by Microsoft Research and the Social Media Research Foundation. NodeXL allows for data visualization, network analysis, and is frequently used in social media research. We seek to visualize the networks created by prominent keyword / concepts expressed in the materials published by hackers. Our approach is that of *co-citation analysis* developed initially by Henry Small[10] and Irena Marshakova-Shaikevich[11] in 1973. We apply the principles of co-citation to the cultural artifacts determined for hacking and hacktivism. The graphs generated will reveal the main keywords / concepts that hackers referred to. In essence, this will reveal the political values of the hacker culture.

The graphs show nodes with different geometrical shapes, including spheres, squares, triangles, and so on. The shapes are irrelevant, but were initially employed for clustering the data as it had the potential to reveal additional details. There are two important nodes (vertices; vertex for singular) that provide *out-degree* edges or *in-degree* edges (connection lines between vertices). The *out-degree* vertex is represented by an item , i.e., a Phrack Pro-Phile, that will send *edges* (connections) to multiple keywords / concepts and establishing *in-degree* vertices (nodes). The size of the out-degree nodes is irrelevant since their purpose is to show basically display the keywords / concepts they contain. However, the in-degree nodes are especially important because their size is determined by the number of *edges* received. It is very important to note that each keyword / concept is unique in one profile, but has duplicates in other profiles. For

[10] Small, Henry, Co-citation in the Scientific Literature: A New Measure of the Relationship Between Two Documents, *in Journal of the American Society of Information Science*, Vol. 24, no. 4, 1973, pp. 265 – 269
[11] Marshakova-Shaikevich, Irena, System of Document Connection Based on References, *Tauchn-Techn*. Inform., Ser. 2, 1973

example, the keyword / concept “information” is recorded just once in the profile of “Tuc” and once in the profile of “Chris Goggans.” Thus, we can observe the popularity of keywords / concepts throughout the established time units. The data visualization and analysis method is supplemented with a close reading of documents in order to include context and hacker attitudes.

The analysis was performed based on time sequencing in time units. For YIPL, we’ve had two time units of one year each and a graph was generated for each of the units and a final graph combining all data for YIPL as well. For Phrack and 2600 we’ve had the following time units:

Phrack I 1986 - 1990	Phrack II 1991 - 1995	Phrack III 1996 – 2000	Phrack IV 2001 – 2005	Phrack V 2006 - 2012

2600 Magazine I. 1984 - 1990	2600 Magazine II. 1991 - 1995	2600 Magazine III. 1996 - 2000	2600 Magazine IV. 2001 - 2005	2600 Magazine V. 2006 - 2011

A graph was generated for each time unit and magazine – a detailed discussion is available in the complete version of the study. For this summary, we will focus just on the final graph generated using the data extracted from YIPL, Phrack, and 2600.

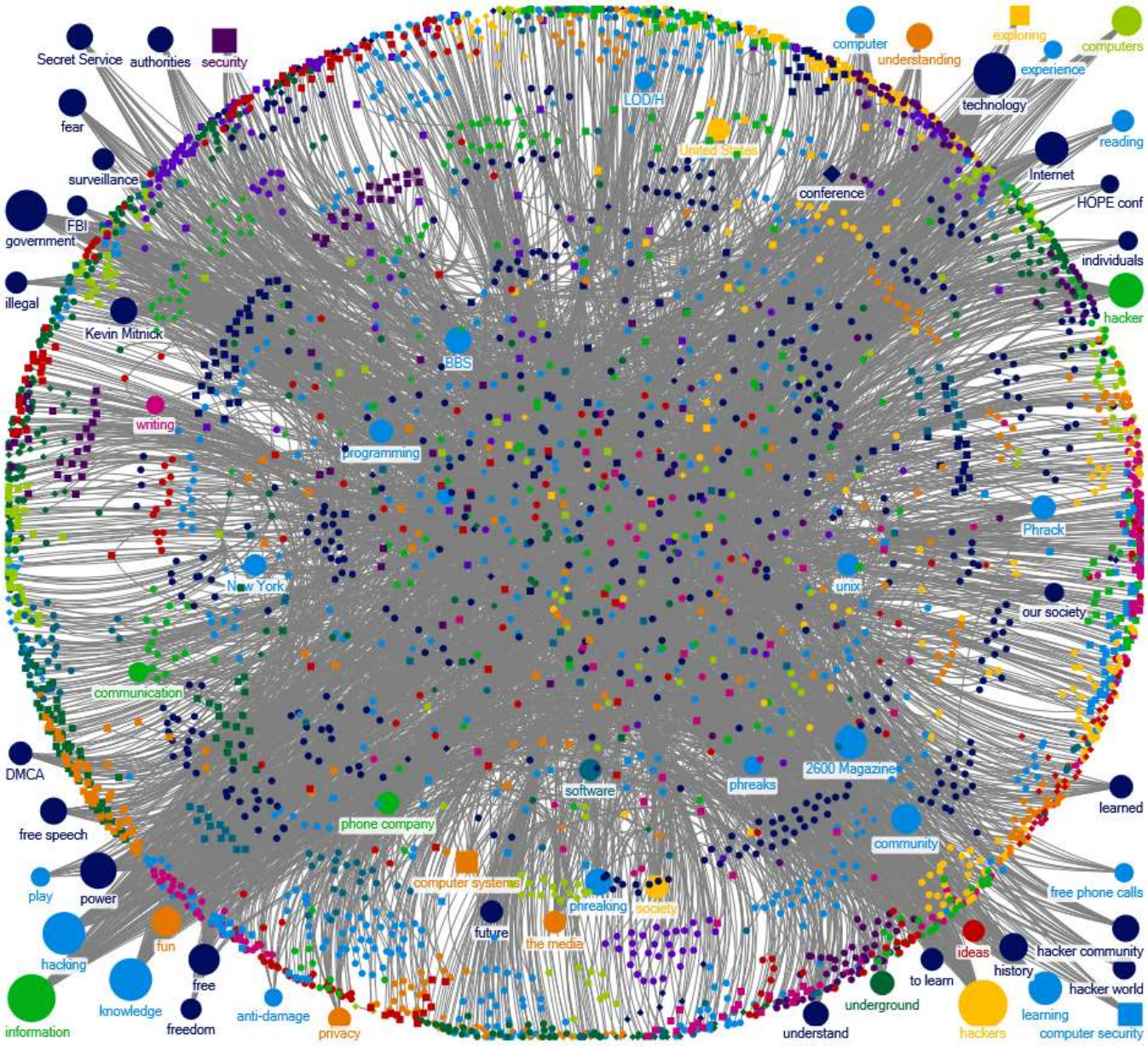

Figure 1. YIPL, Phrack and 2600 Magazine.

The following table shows the top in-degree nodes formed:

Vertex	In-degree
Hackers	69
Information	65
Knowledge	52
Hacking	52
Technology	51
Government	49

Power	38
Hacker	35
Learning	32
Internet	32
2600 Magazine	30
Free	28
Computer	26
Community	26
Fun	25
History	23
Computers	23
Fear	22
Phreaking	21
Kevin Mitnick	21
Hacker world	21
Free speech	21
Secret Service	20
BBS	20
Understanding	19
Authorities	19
Phrack	17
Society	16
Program	16
Learned	16
DMCA	16
United States	15
To learn	15
The media	15
Surveillance	15
Privacy	15
Phone company	15
Future	15
Software	14
Reading	14
New York	14
Illegal	14
Freedom	13
FBI	12
Play	11
Our society	11
Individuals	11
Free phone calls	11
Exploring	11
Phreaking	10
LOD/H	10

Experience	10
Conference	10
Anti-damage	10

The graphs suggests the political preoccupation of the hacker community from 1984 to 2012. In the bottom left corner, we discover the political values of the hacker culture in this moment: “free speech,” “free” and “freedom” as well as “privacy.” The hack is described as “play” or “fun”. We can also discover a strong response to the Digital Millennium Copyright Act or “DMCA” as well as for the Patriot Act. In the bottom right corner, we discover the identity development of hacking expressed in such in-degree nodes as “to learn,” or “learning. In the top right corner, we see that the hacker culture is primarily technology dependent. Here we have in-degree nodes such as “technology,” “computers” and “Internet.” Finally, in the top left corner, we observe the institutions that hackers oppose. We observe such in-degree nodes as “government,” “Secret Service,” and “FBI.”

Based on this data, we observe three concomitantly and interlinked trends emerging. The first direction we name the *technological trend*. This trend is represented by nodes such as “pay phone” that shows that the primary aspect of the hacker culture is its dependence on technology. The second trend we name the *learning trend* that recognizes the hackers’ desire to seek out information and learn how to overcome the obstacles given by the system. It is represented by in-degree nodes as “information” and “learning” as well as “knowledge” and other similar concepts. The third trend we understand as the *political active trend*. This trend is represented by nodes that have a political connotation such as “freedom” or “surveillance” or “authorities” including government institutions and agencies such as “FBI” or “Secret Service.” These trend will persist in the case of hacktivism as well.

Hacking, the data suggests, or “the hack” is championing individual freedoms and the development of tools, software, that would aid the individual or groups in their political purposes. It is a form of play-exploration that with the ultimate goal of acquiring knowledge about systems. Therefore, we can suggest that hacking is *ludic*. Following the framework of strategic culture, we conclude that the political values of the hacker culture lie within individual freedoms: freedom of speech, freedom of association, freedom of information, and privacy.

In the next chapter, *Hacking*, we explore the activity of politically active hacking groups through our research framework of play and strategic culture. The definitions of hacktivism try to accommodate the technological aspect of hacking and the "offline" political activism. In many ways, we agree with this definition, but we also suggest that hacktivism is the manifestation of political hacker values that we have discovered in the previous chapter. Steven Levy in *Hackers: Heroes of the Computer Revolution* proposes a set of principles that political hacking follows.[12] The principles have been divided into three groups:

Political Principles	Nonpolitical Principles	Grey Area Principles
Unlimited and unrestricted access to computers that hold information about the workings of the world.	Hackers should be judged based on merit and not bogus criteria such as degrees, age, rage, or position.	Hackers can create art and beauty on computer.
Unrestricted access to information. Information wants to be free.	Hackers can create art and beauty on computer.	Computers can change your life for the better. Hacking is innovation with positive outcomes.
Mistrust Authority – Promote Decentralization. Monopolies of any kind are not tolerated, especially "monopolies on knowledge."	Computers can change your life for the better. Hacking is innovation with positive outcomes.	

The next section is a brief discussion on the *Methods* of hacktivism. It becomes clear that the most common method used is the denial of service attack. This method is also problematic because not all groups consider it to be a legitimate method for digital protest. Denial of Service, or DOS, is simple in principle. The idea behind it is to send overwhelm the target server with requests to make it shut down temporarily. The Electronic Disturbance Theater was among the

[12] Levy, Steven, *Hackers*, O'Reilly Media, 2010, 25th edition

first group who have developed software, *Floodnet*, with this purpose. DOS operations were used by the EDT against the Mexican government in support of the Zapatista movement. The EDT is also the group that has provided a theoretical justification, based on the *civil disobedience* by Henry David Thoreau. The Cult of the Dead Cow, however, had a different view. They considered denial of service a form of censorship. Instead, they would produce software designed to allow individuals and groups to overcome the possible censorship of institutions, corporations, and governments. Anonymous would develop software exclusively for operations. In this case, they have developed their own, updated, version of *Floodnet*, that was used for operations against PayPal, Mastercard, Sony and so on.

The cultural artifacts selected for this part of our study are the publication efforts of the aforementioned groups. Their political views should become visible in the press releases, statements, and books that they have published. In the case of Anonymous, given the nature of the group, it is quite difficult to establish the validity of their publications. Instead, we have chosen to analyze a book published recently that supposedly has the voluntary contributions of individuals who affiliate themselves with the hacker group.

Graph generation and interpretation method. The principles for graph generation and of interpretation are similar to the previous case. The difference is that we have generated one single graph for the entire group, i.e. one graph for Anonymous, and one graph to visualized the combined data from the other graphs. A detailed discussion can be found in the full version of this study. For now, we will focus just on the graph generated for all the data of hacktivism.

4.2.

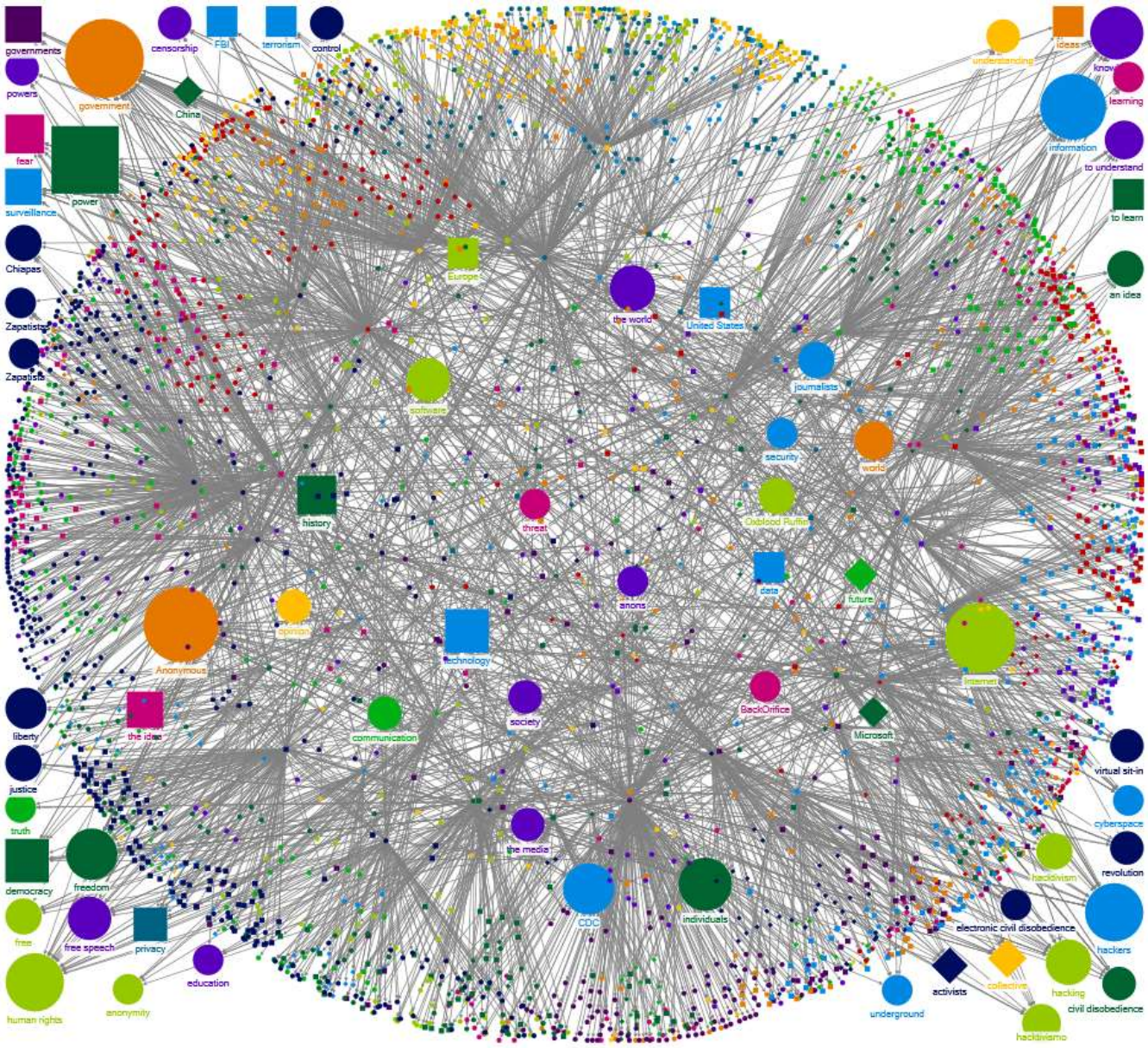

Figure 2. The graph combines the data from all hacktivist cultural artifacts.

The following table shows the most prominent nodes:

Vertex	In-degree
Anonymous	30
Internet	26
Power	24
Information	23
Human rights	18
Hackers	18
Individuals	15
Freedom	14
CDC	14
The world	11
Technology	10
Software	10
Free speech	10
Democracy	10

We can observe a pattern of in-degree nodes that is quite similar to the previous graph. However, the graph and in-degree nodes table show a more nuanced landscape of the values of political hacking. In the bottom left corner we see the in-degree nodes referring to "free" and "free speech" that have now become traditional values of the hacker culture. Hackers are also preoccupied with issues of "privacy," "truth" and "education." We can also discover in-degree nodes such as "justice," "liberty." In the top left corner, we can observe a pattern emerging for the institutions that hacker oppose. The in-degree node "government" is present again. Furthermore, they are interested in issues of "surverillance," and "censorship" as well as forms of "control and the political "power."

Based on the data available, we propose a typology of hacktivism grounded on their interpretation of hacktivism. First we have the *intellectual* approach of the ludic digital protest exemplified by EDT. The essential political values of the hacktivists are expressed in terms of "human rights" and in support of various forms of "freedom." The second, in the case of Cult of the Dead Cow, is the *productive* approach of the ludic digital protest. CDC developed software such as Camera/Shy or Torpark, or BackOrifice, giving individuals and groups the tools to protect themselves against censorship and breaches of privacy. Finally, we have the *action*-oriented aspect of the ludic digital protest. The *trend* in this case moves towards the political

active trend but with the exception of CDC where we have a balance shared with the technological trend. It is important to note that in all cases, the technological trend and the learning trend have never disappeared completely. These trends evolve concomitantly and are interlinked rather than separate. Overall, we conclude that hacktivism is a political manifestation of essential hacker values.

In the next chapter we provide the graph generated for the entire collection of cultural artifacts and conclude our study.

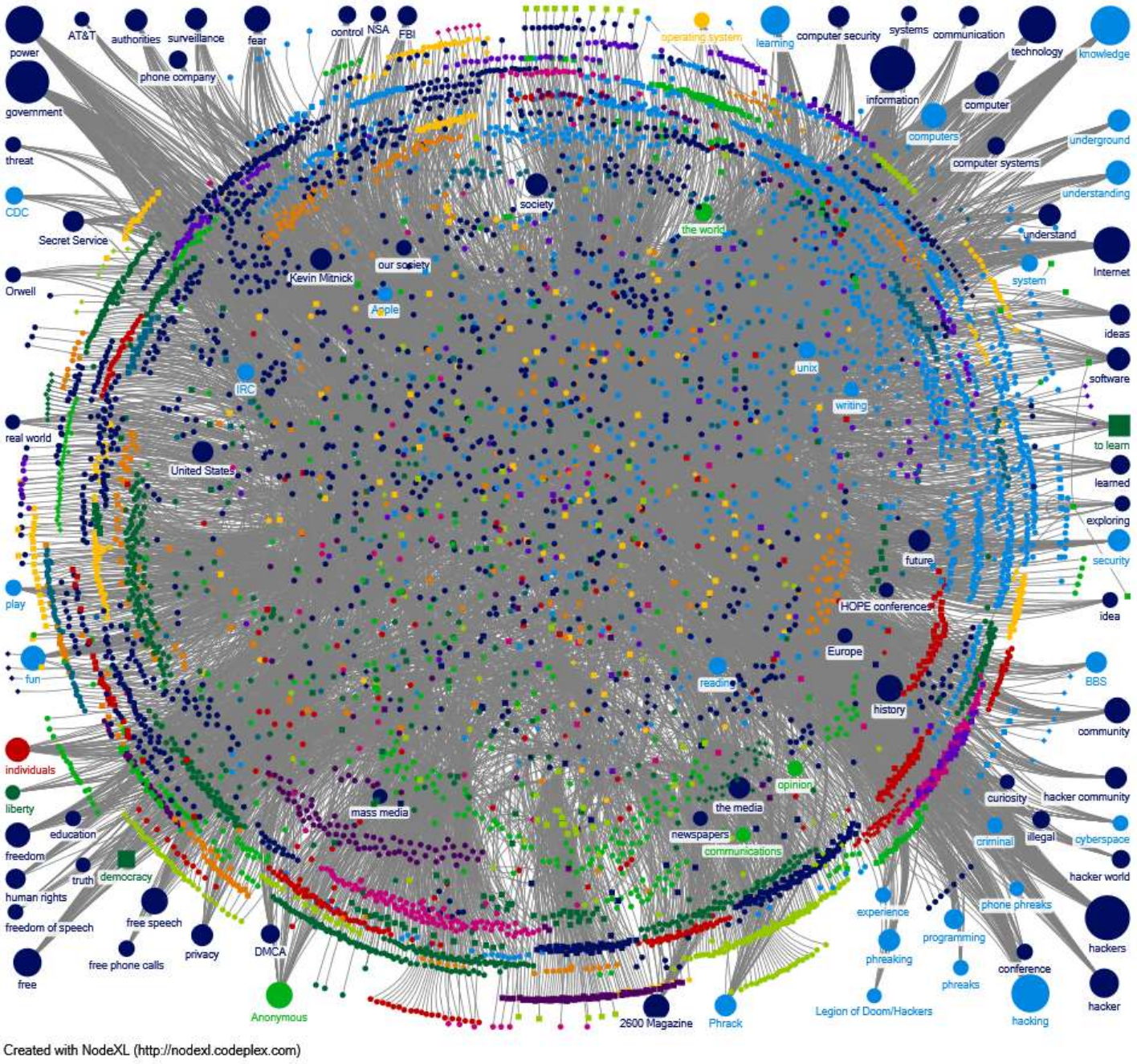

Figure 3. Data visualized from all cultural artifact sources.

The graph generated above is directed and presents a total of 5876 vertices and a total of 11043 edges with 8769 unique edges and 2274 edges with duplicates. The table below lists the top in-degree nodes.

Vertex	In-degree
Information	88
Hackers	87
Phrack	21
CDC	14
Conference	12
Underground	22
Security	22
Experience	11
Free	35
Free phone calls	12
Phreaks	11
Government	82
Cyberspace	11
Hacker	37
Knowledge	67
Hacking	63
Programming	18
Phone phreaks	10
Internet	58
Orwell	11
Power	62
Computers	28
Fun	27
Operating system	11
Learning	37
To learn	20
Threat	11
System	13
Human rights	18
History	31
Control	14
Software	24
United States	20
Real world	10
Technology	61
Play	12
Surveillance	21
FBI	17
Europe	10
Democracy	13
Free speech	31
Computer security	20
The media	21
The world	15

Privacy	21
Future	21
Systems	11
Anonymous	31
Freedom	27
Individuals	26
Liberty	10
Truth	10
Fear	30
Communication	18
Ideas	19
Education	11
Curiosity	10
Computer	26
Understand	22
Mass media	10
IRC	13
Opinion	11
Authorities	22
Freedom of speech	11
Society	22
Communications	10
Criminal	11
NSA	11
Learned	17
Understanding	26
Newspapers	10
Community	29
Phreaking	21
2600 Magazine	30
Legion of Doom/Hackers	10
BBS	20
Phone company	15
Reading	15
Apple	10
Idea	10
AT&T	10
Computer systems	14
Unix	14
Exploring	11
Secret Service	20
Writing	10
Illegal	14
Kevin Mitnick	21
Our society	11

Hacker world	15
Hacker community	21
DMCA	16
HOPE conferences	10

We can easily observe that a pattern was developed. That pattern identifies the political values of the hacker culture. Thus, we can observe a "residual degree of continuity" in the hacker values from YIPL to Anonymous. The pattern consists of in-degree nodes such as "government" and "free." Also, as we move more into hacktivism instead of hacking, we observe that hackers appreciate other concepts such as "liberty," "human rights," "power," and "free speech." Thus, the pattern points towards *the hacker spirit* that stands, if it has to, against the political authority and powers of government. The definition that we propose for hacktivism is the following:

> Hacktivism is a ludic form of digital protest animated by traditional hacker values to organize online operations and produce software that enable individual users or organized groups to protest for human rights in cyberspace.

The manifestations of the hacker culture are not without socio-political consequences. Our approach has opened the door for new interpretations of traditional concepts such as sovereignty, political border, security, and even the nation state. In the chapter *On the Consequences of Hacking* we reflect upon this impact. In the chapter, we acknowledge that there is something specific brought into play, *the hacker spirit*. This concept has emerged in our data-driven text analysis of the identified cultural artifacts, especially in 2600 Magazine. It is not meant to describe the hacker culture, nor to define it. It is the *Geist* of the hacker culture. Through it, it produces a change of mentality and a distinctively incipient philosophy that hackers have unknowingly initiated.

Hacking does not know a geographical imperative. The consequence being that traditional institutions find themselves helpless in dealing with real cyber threats. Thinking of our Western culture in terms of strategic culture, we observe that we, too, have a series of cultural artifacts that define our perspective on security: Clausewitz, Jomini, and others. Since concepts of sovereignty, political borders, and even the nation state, become less relevant, the hacker spirit can allow for the development of a new methodology to address cyber threats that, sometimes, require distancing from the traditional research methods. For example, cyber threats

should be viewed not only as nonconventional, nonlinear, or nontraditional forms of attack, but as the illicit knowledge acquisition of the target system, mastery over the target system through originality and simplicity. In other words, they should be acknowledged as a ludic form of hacking, even if the consequences are not positive. The extended discussion is available in the full version of this study.

Clausewitz, Jomini, and every military scholar, perhaps except Sun Zi, view war in terms of the physical power to subdue the enemy. However, we discover single individuals that do not require the resources of traditional military institutions, but have the potential to cause a tremendous amount of problems. Cyber threats are real and important, but the hacker spirit proposes a new approach of addressing them that requires suspending the traditional Western mentality of levels of authority and power. Cyberspace is the playground for such a paradigm change. Due to the potential innovative aspect of the play of hacking, the software solutions within the tensions of cyber security, would probably benefit individuals and secure the nation state. Until then, hacking can be an instrument for power, but, simultaneously, is also a power itself and for itself.