UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/383,024	09/04/2014	Joshua Charles Neil	1620.0006	8291

147210 7590 12/20/2018
LeonardPatel PC
Triad National Security, LLC
9891 Irvine Center Drive
Suite 100
Irvine, CA 92618

EXAMINER
DAVIS, ZACHARY A

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
12/20/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@leonardpatel.com
docket@lanl.gov
mleonard@leonardpatel.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JOSHUA CHARLES NEIL, MELISSA TURCOTTE, and
NICHOLAS ANDREW HEARD

Appeal 2018-003607
Application 14/383,024
Technology Center 2400

Before JOHN A. JEFFERY, DENISE M. POTHIER, and
JUSTIN BUSCH, *Administrative Patent Judges*.

POTHIER, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants[1,2] appeal under 35 U.S.C. § 134(a) from the Examiner's decision to reject claims 1–5, 8–10, 12–17, 19, and 20. Appeal Br. 13–50. Claims 6, 7, 11, and 18 have been canceled. *See* Appeal Br. 6. We have jurisdiction under 35 U.S.C. § 6(b). We affirm.

[1] Throughout this opinion, we refer to the Final Action (Final Act.) mailed May 5, 2017; the Appeal Brief (Appeal Br.) filed October 4, 2017; the Examiner's Answer (Ans.) mailed December 22, 2017; and the Reply Brief (Reply Br.) filed February 20, 2018.
[2] The real party in interest is listed as Los Alamos National Security, LLC. Appeal Br. 4.

Invention

"Detecting attacks by multiple attackers, whether human or automated systems (e.g., botnets)[,] is of increasing importance in interest in computer security." Spec. ¶ 4. But "methods that address coordinated attacks on internal networks have not been addressed." *Id.* ¶ 7. Appellants' invention relates to "detect[ing] anomalies to identify coordinated group attacks on internal computer networks." *Id.* ¶ 8.

Illustrative claim 1 is reproduced below:

> 1. A computer-implemented method for detecting coordinated group attacks on a network, comprising:
>
> determining, by a computing system, an anomaly graph of the network, the anomaly graph comprising nodes, edges, and an indegree of the nodes;
>
> designating, by the computing system, nodes with an indegree of at least two as potential targets;
>
> designating, by the computing system, nodes with no incoming connections as potentially compromised nodes; and
>
> outputting, by the computing system, an indication of the designated potentially compromised nodes as potentially associated with a coordinated attack on the network when the potentially compromised nodes connect to at least one of the same potential target nodes, wherein
>
> for a p-value threshold $T \in (0,1)$, the anomaly graph $S_t = (V_t^S, E_t^S)$ of the network is formed from the edges that have a positive p-value below the threshold:
>
> $$E_t^S = \{(i,j) \in E_t \mid p_{ij,t} < T\}$$
>
> $$V_t^S = \{i \in V_t \mid \exists j \neq i \in V_t \text{ s.t. } (i,j) \in E_t^S \; or \; (j,i) \in E_t^S\}$$
>
> where E_t^S is a set of edges in S_t, V_t^S is the set of nodes in S_t, and $p_{ij,t}$ is the p-value for a given edge $(i,j) \in E_t$.

Appeal Br. 52–53 (Claims App'x).

The Rejection

Claims 1–5,[3] 8–10, 12–17, 19, and 20 are rejected under 35 U.S.C. § 101 as being directed to patent ineligible subject matter. Final Act. 9–13; *see also* Ans. 3–11.[4]

CONTENTIONS

Appellants argue claims 1–5, 8–10, 12–17, 19, and 20 as a group. *See* Appeal Br. 25–50; Reply Br. 2–19. We select claim 1 as representative. *See* 37 C.F.R. § 41.37(c)(1)(iv).

Regarding representative claim 1, the Examiner finds the claims are directed to, among other things, "the abstract idea of . . . determining a graph based on p-values and using that graph data to categorize nodes." Final Act. 4; *see also* Final Act. 9–10. The Examiner further finds the recited steps involve obtaining and analyzing data pertaining to network computing system activities. Ans. 4–5. The Examiner further states the claim elements taken individually or as an ordered combination do not include additional elements that amount to significantly more than the abstract idea. Final Act. 10–11. The Examiner determines that the claim recites no more than a generic computer to perform generic computer functions that are well-understood, routine, and conventional activities previously known in the industry. *Id.*

[3] Claim 6 has been canceled and no longer forms part of the § 101 rejection. Ans. 3.

[4] The rejection based on 35 U.S.C. § 112 second paragraph presented in the Final Acton (Final Act. 14–18) has been withdrawn (Ans. 3).

Appellants argue that the claimed invention is not directed to an abstract idea because cybersecurity technology by its very nature is an improvement in computer functionality that arises out of problems occurring in networked computing systems (Appeal Br. 34), and "the claimed invention presents a novel way of detecting coordinated group attack behavior in a network" (Reply Br. 4). Appellants add that even if the claimed invention is directed to an abstract idea, the claims nevertheless recite additional elements that add significantly more to the abstract idea by, among other things, providing specific, discrete implementations of advanced cybersecurity technology. Appeal Br. 47.

ISSUE

Under § 101, has the Examiner erred in rejecting claim 1 by finding that the claim is directed to judicially excepted, patent ineligible subject matter?

ANALYSIS

Based on the record before us, we find no error in the Examiner's rejection of independent claim 1. Under § 101, a patent may be obtained for "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." The Supreme Court has "'long held that this provision contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable.'" *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2354 (2014) (quoting *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107, 2116 (2013)). The Supreme Court in *Alice* reiterated the two-step framework previously set forth in *Mayo Collaborative Services v. Prometheus Laboratories, Inc.*, 566 U.S. 66 (2012), "for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts." *Alice*, 134 S. Ct. at 2355. First, "determine whether the claims at issue are directed to a patent-ineligible concept," such as an abstract idea. *Id.* Abstract ideas may include, but are not limited to, fundamental economic practices, methods of organizing human activities, an idea of itself, and mathematical formulas or relationships. *Id.* at 2355–57. If so, "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements" add enough to transform the "nature of the claim" into "significantly more" than a patent-ineligible concept. *Id.* at 2355, 2357 (quoting *Mayo*, 566 U.S. at 79); *see Affinity Labs of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016).

MAYO/ALICE STEP 1

Step one in the *Mayo/Alice* framework involves looking at the "focus" of the claims at issue and their "character as a whole." *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016); *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016). "The 'abstract idea' step of the inquiry "calls upon us to look at the 'focus of the claimed advance over the prior art' to determine if the claim's 'character as a whole' is directed to excluded subject matter." *Affinity Labs*, 838 F.3d at 1257 (citing *Elec. Power Grp.*, 830 F.3d at 1353).

Claim 1's preamble recites "[a] computer-implemented method for detecting coordinated group attacks on a network." Appeal Br. 52 (Claims App'x). The method includes four steps—(A) determining a network anomaly graph having nodes, edges, and nodes' indegrees[5] ("determining . . . an anomaly graph of the network . . . comprising nodes, edges, and an indegree of the nodes" and "the anomaly graph . . . is formed from the edges that have a positive *p*-value below [a threshold *T*]" ("step (A)")); (B) separately designating (1) nodes with an indegree of at least two as potential targets, and (2) nodes with no incoming connections as potentially compromised nodes ("designating . . . nodes with an indegree of at least two as potential targets; [and] designating . . . nodes with no incoming connections as potentially compromised nodes" ("steps (B)(1) and (B)(2)")); and (C) outputting an indication of the designated potentially compromised nodes as potentially associated with a coordinate attack when they connect to a same potential target node ("outputting . . . an indication of the designated potentially compromised nodes as potentially associated with a coordinated attack on the network when the potentially compromised nodes connect to at least one of the same potential target nodes" ("step (C)")). *Id.* at 52–53 (Claims App'x).

We agree with both the Examiner and Appellants that claim 1's focus is directed to "determining a graph based on p-values and using that graph data to categorize nodes" (Final Act. 4) as well as "detecting coordinated group attacks on a network" using a graph (*see* Appeal Br. 34). *See Apple, Inc. v. Ameranth, Inc.*, 842 F.3d 1229, 1240–41 (Fed. Cir. 2016) (determining "[a]n abstract idea can generally be described at different levels of abstraction."). That is, claim 1's preamble indicates the claim is

[5] The Specification describes a node that receives no incoming connections as a node with zero indegree and nodes 7 and 8 in Figures 1A and 1B as having an indegree of two or more. Spec. ¶ 30, Figs. 1A–B.

"for detecting coordinated group attacks on a network," as Appellants discuss, and claim 1's body focuses on determining a graph and using the graph's data to categorize nodes to detect coordinated group attacks, as the Examiner discusses. Moreover, the Specification supports this characterization of claim 1. That is, the Specification describes determining a graph of network activity using a formula and detecting coordinated attacks on internal networks through anomalies based on the graph. Spec. ¶¶ 3, 8–9, 25–29.

Regardless of claim 1's characterization, the steps in claim 1 are directed to excluded subject matter, including one or more abstract ideas for the reasons that follows.

There is no definitive rule in determining what constitutes an "abstract idea." *Enfish*, 822 F.3d at 1334 (citing *Alice*, 134 S. Ct at 2357). We need only look to other decisions where similar concepts were previously found abstract by the courts. *See Amdocs (Isr.) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1294 (Fed. Cir. 2016); *see also Enfish*, 822 F.3d at 1334–35. The Examiner concludes the claims are directed to two separate, abstract ideas. First, the Examiner concludes the claimed anomaly graph and resulting determination of the anomaly graph (i.e., step (A) outlined above) is similar to the mathematical algorithms determined abstract in *Gottschalk v. Benson*, 409 U.S. 63 (1972) and *Parker v. Flook*, 437 U.S. 584 (1978). Final Act. 9–10; Ans. 4. Second, the Examiner concludes the claimed steps of designating and outputting (i.e., steps (B)(1), (B)(2), and (C) outlined above) are similar to the abstract ideas identified in *Digitech Image Technologies, LLC v. Electronics for Imaging, Inc.*, 758 F.3d 1344 (Fed. Cir. 2014) and *Electric Power Group*. Final Act. 10; Ans. 5.

The Abstract Idea(s)

Courts have found claims with mathematical algorithms can be directed to an abstract idea. *See Benson*, 409 U.S. at 67 (a "method for converting numerical information from binary-coded decimal numbers into pure binary numbers . . . [is merely a series of mathematical calculations or mental steps, and does not constitute a patentable] 'process'"); *Flook*, 437 U.S. at 594–96 (rejecting as ineligible claims directed to the use of an algorithm to calculate an updated "alarm-limit value" for a catalytic conversion process variable, and updating the limit with the new value). "Yet it is equally clear that a process is not unpatentable simply because it contains a law of nature or a mathematical algorithm." *Flook*, 437 U.S. at 590.

Turning to claim 1, the anomaly graph based on p-values from step (A) outlined above involves a mathematical algorithm. Claim 1's step (A) recites

> determining . . . an anomaly group of the network . . .[,]
>
> the anomaly graph S_t, = (V_t^S, E_t^S) of the network is formed from the edges that have a positive p-value below the threshold:
>
> $$E_t^S = \{(i,j) \in E_t \mid p_{ij,t} < T\}$$
> $$V_t^S = \{i \in V_t \mid \exists j \neq i \in V_t \text{ s.t. } (i,j) \in E_t^S \; or \; (j,i) \in E_t^S\}$$
>
> where E_t^S is a set of edges in S_t, V_t^S is the set of nodes in S_t, and $p_{ij,t}$ is the p-value for a given edge $(i,j) \in E_t$.

Appeal Br. 52–53 (Claims App'x). Specifically, claim 1's graph is formed by computing a mathematical algorithm.

Appellants contend claim 1 is not analogous to the claims in *Benson* and *Flook*, but rather the claims in *Diamond v. Diehr*, 450 U.S. 175 (1981). According to Appellants, claim 1 does not seek solely to patent a mathematical algorithm, but rather to cover a process that detects a computer network's potentially anomalous behavior indicative of a group attack using a mathematical algorithm. Appeal Br. 27. Appellants contend "the providing of the indication itself [(e.g., step (C))] constitutes a practical application of the algorithm." Appeal Br. 29. We determine the comparison to *Diehr* does not hold and conclude claim 1 is more analogous to the claims in *Flook*.

The claims in *Diehr* were directed to a process for curing synthetic rubber. Notably, the claims recited a series of steps (e.g., the loading of a mold with raw, uncured rubber, closing the mold, constantly determining the mold temperature, constantly recalculating the cure time, and automatically opening the press at the proper time) that together provided a significant and novel practical application of the well-known Arrhenius equation and transformed uncured synthetic rubber into a new state or thing. *See Diehr*, 450 U.S. at 184–87. "In contrast [with *Benson* and *Flook*], the respondents [in *Diehr*] do not seek to patent a mathematical formula. Instead, they seek patent protection for a process of curing synthetic rubber." *Id.* at 187.

We do not see that situation here. Unlike the process claimed in *Diehr*, which was directed to a specific industrial process, i.e., "a physical and chemical process for molding precision synthetic rubber products," *id.* at 184, Appellants' claims merely recite a method for designating specific nodes in an anomaly graph and outputting an indication when any designated node exhibits a specific characteristic. At best, claim 1's preamble provides a practical application for the mathematical algorithm in step (A). But a mere recitation of a practical application for an abstract idea is insufficient to transform an abstract idea into an inventive concept. *See*

CyberSource Corp. v. Retail Decisions, Inc., 654 F.3d 1366, 1371 (Fed. Cir. 2011) ("The Court [in *Flook*] rejected the notion that the recitation of a practical application for the calculation could alone make the invention patentable . . . .").

Notably, the claims in *Flook* included computing and adjusting an alarm limit related to a catalytic chemical conversion process. *Flook*, 437 U.S. at 586 (App'x). Despite the claims not covering every application of the formula and not preempting all uses of the formula (*id.* at 586, 589–90), the Court determined *Flook*'s claims "cover any use of respondent's formula for updating the value of an alarm limit on any process variable involved in a process comprising the catalytic chemical conversion of hydrocarbons." *Id.* at 586. In essence, the Court concluded *Flook*'s claims are directed to an abstract idea. *Id.* at 586–89.

Similarly, the instant claims are directed to determining nodes of interest (e.g., those having a specific indegree number or no incoming connections) using a formula and outputting an indication (e.g., nodes) of some of the determined nodes associated with a coordinated attack. Appeal Br. 52 (Claims App'x). Claim 1 does not cover every application (e.g., reciting a method "for detecting coordinated group attacks"), but does cover any use of its formula to output an indicator of potentially comprised nodes in a process for detecting coordinated group attacks. Like *Flook*'s claims, claim 1 is therefore directed to at least one abstract idea. *See* Final Act. 7, 10 (citing *Flook* when addressing the abstract idea); *see also* Ans. 4, 6, 11 (same).

Additionally, a claimed method is directed to "an abstract idea because it describes a process of organizing information through mathematical correlations and is not tied to a specific structure or machine." *Digitech*, 758 F.3d at 1350. The claims in *Digitech* were directed to generating profiles for "a device in a digital image reproduction system for capturing, transforming or rendering an image." *Id.* at 1351. But, "[w]ithout additional limitations, a process that employs mathematical algorithms to manipulate existing information to generate additional information is not patent eligible." *Id.*

Similarly, claim 1's steps (A) through (C) outlined above involve organizing information through a mathematical correlation, taking existing information (e.g., that related to "the network"), and using a mathematical algorithm (e.g., "an anomaly graph of the network") to create additional information (e.g., "designating . . . nodes with an indegree of at least two as potential targets," "designating . . . nodes with no incoming connections as potentially compromised nodes," and "outputting . . . an indication of the designated potentially compromised nodes as potentially associated with a coordinated attack on the network . . . "). Appeal Br. 52 (Claims App'x). Like the claims in *Digitech*, claim 1 creates additional information and is still directed to an abstract idea. *See* Final Act. 7, 10 (citing *Digitech* when addressing the abstract idea); *see also* Ans. 4, 11 (same).

Courts have also found steps of gathering, analyzing, manipulating, and comparing information and displaying results are directed to an abstract idea. *See Elec. Power Grp.*, 830 F.3d at 1354 (determining the claims were directed to an abstract idea of gathering and analyzing information of a specified content and displaying results), *cited in* Final Act. 5, 7, and 10 and Ans. 4–5, 8, and 11; *see also Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014*)* (determining the claims were directed to the abstract idea of collecting data using a scanner, recognizing specific information within a collected dataset, and storing the recognized data in memory); *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1366–67 (Fed. Cir. 2018) (stating the claims were directed to an abstract idea of parsing and comparing information akin to collecting and recognizing data and classifying data in an organized manner).

Likewise, claim 1's steps (A) through (C) outlined above involve gathering information (e.g., that from "the network"), analyzing or comparing information (e.g., "determining . . . an anomaly graph of the network," "designating . . . nodes with an indegree of at least two as potential targets," and "designating . . . nodes with no incoming connections as potentially compromised nodes"), and generating results (e.g., "outputting . . . an indication of the designated potentially compromised nodes as potentially associated with a coordinated attack on the network when the potentially compromised nodes connect to at least one of the same potential target nodes"). Appeal Br. 52 (Claims App'x). Moreover, even when such information is limited to particular content, it is well-settled that such steps, such as collecting certain information, is within the realm of abstract ideas. *Elec. Power Grp.*, 830 F.3d at 1353.

Also, but for the recitation of the "computing system" in claim 1, steps (A) through (C) could be performed as mental steps, or with the aid of pen and paper. *See CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1375 (Fed. Cir. 2011) ("That purely mental processes can be unpatentable, even when performed by a computer, was precisely the holding of the Supreme Court in *Benson*."); *Elec. Power Grp.*, 830 F.3d at 1354 ("analyzing information by steps people go through in their minds, or by mathematical algorithms, without more, as essentially mental processes within the abstract-idea category.'"). We disagree with Appellants that a human could not detect "connections between computing systems" (Appeal Br. 38). That is, after determining an anomaly graph, a human could observe connections between nodes. Appeal Br. 52 (Claim App'x).

Appellants assert the claims in *Digitech* and *Electric Power Group* "can accurately be characterized as merely organizing and reordering provided data, or storing data in a profile." Appeal Br. 31. Appellants argue their claims differ from the claims in *Digitech* and *Electric Power Group* because the recited anomaly graph is a newly created structure not modified from a previous representation. *Id.* Appellants further argue the recited anomaly graph did not previously exist, unlike the available information that is collected, analyzed, and displayed in *Electric Power Group*'s claims. Reply Br. 9. We are not persuaded. Contrary to Appellants' argument (App. Br. 31; Reply Br. 9), the recited network—not the recited anomaly graph—is available for collecting and analyzing related information to determine the graph, or used to create additional information (e.g., the anomaly graph) and nodes of interest like that in the claims in *Digitech*. Similarly, claim 1's steps are like those in *Electric Power Group*, which collect data from an electrical power grid's data and detect, analyze, and display additional information using the collected power grid data. *See Elec. Power Grp.*, 830 F.3d at 1351–52.

Appellants also argue their claims differ from the claims in *Cyberfone Sys., LLC v. CNN Interactive Grp.*, 558 F. App'x 988 (Fed. Cir. 2014) (unpublished) and *SmartGene Inc. v. Advanced Biological Labs. SA*, 555 F. App'x 950 (Fed. Cir. 2014) (unpublished). Appeal Br. 30–32. Based on our discussion concerning *Flook*, *Digitech*, and *Electric Power Group*, we need not address these non-binding opinions.

Enfish, Finjan, and McRO

Appellants attempt further to compare claim 1 to the claims in *Enfish*, asserting "by its very nature, cybersecurity technology, such as software that detects the potential presence of multiple attackers engaging in a coordinated attack on a network, is itself an improvement in computer functionality that arises out of problems occurring in networked computing systems." Appeal Br. 36. We disagree.

At the outset, we note narrowing a field in claim 1 to cybersecurity technology does not make the claim any less abstract. *See OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1362–63 (Fed. Cir. 2015) ("[T]hat the claims do not preempt all price optimization or may be limited to price optimization in the e-commerce setting do not make them any less abstract.").

The invention of *Enfish* was "directed to an innovative logical model for a computer database." *Enfish*, 822 F.3d at 1330. In contrast to prior-art databases that were based upon a relational model, *Enfish*'s invention was directed to a self-referential model wherein all information of the database appears in a single table, and given rows of the table reference other rows of that same table. *Id.* at 1332–33. The method of Appellants' claim 1, by contrast, is not directed to "an improvement to computer functionality itself." *Id.* Rather, claim 1 carries out "tasks for which a computer is used in its ordinary capacity," *id.*; specifically, the claimed steps involve determining an anomaly graph (e.g., computing a formula) to generate information, designating nodes of the anomaly graph (e.g., computing values to determine nodes), and outputting an indication (e.g., outputting values/nodes) upon detecting an anomaly graph possesses specific characteristics.

Nor are we persuaded by Appellants' comparison of claim 1 to the claims found patent eligible in *Finjan, Inc. v. Blue Coat Systems, Inc.*, 879 F.3d 1299 (Fed. Cir. 2018). *See* Reply Br. 2–17. In *Finjan*, the court held that claims directed to a behavior-based virus scan constituted an improvement in computer functionality over the "traditional, 'code-matching' virus scans." *Id.* at 1304. Instead of looking for the presence of known viruses, "behavior-based" scans analyze a downloadable's code and determine whether the code performs potentially dangerous or unwanted operations, thus, enabling more flexible and nuanced virus filtering. *Id.* The court determined that the claimed method employs a new kind of file, allows access to be tailored for different users, and allows the system to accumulate and use newly available, behavior-based information about potential threats. *Id.* at 1305. Based on these findings, the court determined that the claims are "directed to a non-abstract improvement in computer functionality, rather than the abstract idea of computer security writ large." *Id.* "Here, the claims recite more than a mere result. Instead, they recite specific steps—generating a security profile that identifies suspicious code *and* linking it to a downloadable—that accomplish the desired result." *Id.* (emphasis added).

Unlike the claims of *Finjan*, Appellants' claims are not directed to employing a newly generated file that contains a security profile identifying suspicious code in the received downloadable, thereby constituting an improvement in computer functionality. *Finjan*, 879 F.3d at 1304–05. Although claim 1 may generate an indicator of "potentially comprised nodes as potentially associated with a coordinated attack," this claim recites outputting an indication when certain nodes connect to other nodes— a mere desired result. This claim fails to employ a newly generated file containing security profile data in a downloadable and does not use a newly generated file to enable a computer security system to do things it could not do before—the specific steps to accomplish the result. Thus, unlike the claims in *Finjan*, claim 1 does not improve a computer's functionality.

We further are not persuaded by Appellants' comparison of claim 1 to the claims found patent eligible in *McRO, Inc. v. Bandai Namco Games America Inc.*, 837 F.3d 1299 (Fed. Cir. 2016). We determine Appellants' claims are more akin to the claims the Federal Circuit found ineligible in the previously discussed cases than the claims in *McRO*, which address "a specific asserted improvement in computer animation" and "us[ing] a combined order of specific rules that renders information into a specific format that is then used and applied to create desired results: a sequence of synchronized, animated characters." *McRO*, 837 F.3d at 1314–15.

For the foregoing reasons, we determine claim 1 is directed to one or more abstract ideas.

MAYO/ALICE STEP 2

Next, we consider the elements of claim 1 both individually and as an ordered combination to determine whether the additional elements add enough to transform the claim into significantly more than a patent-ineligible concept. Step two in the *Mayo/Alice* framework involves the search for an "inventive concept." *Alice*, 134 S. Ct. at 2355; *Elec. Power Grp.*, 830 F.3d at 1353. An "inventive concept" requires more than "well-understood, routine, conventional activity already engaged in" by the relevant community. *Rapid Litig. Mgmt. Ltd. v. CellzDirect, Inc.*, 827 F.3d 1042, 1047 (Fed. Cir. 2016) (quoting *Mayo*, 566 U.S. at 79–80).

To recap, we determine above that the functions concerning the steps (A) through (C) outlined above are not additional elements to the abstract ideas. As previously discussed, these steps are drawn to the abstract ideas of a mathematical relationship as well as gathering, analyzing, and generating additional information based on the mathematical relationship.

The Examiner concludes under step two in the *Mayo/Alice* framework that acclaim 1's generically recited computer implementation of steps (A) through (C) outlined above does not add "significantly more" to the abstract ideas embodied in the claims. Final Act. 10–11. Instead, the additionally claimed "computer system" in claim 1 fails to transform the claim's nature into a patent-eligible concept, but rather is used as a tool to perform the claim's steps. *See Alice*, 134 S. Ct. at 2358 (holding "the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention"). Moreover, claim 1 does not recite a transformation or a practical application like the claimed invention in *Diehr* as previously discussed. *See Diehr*, 450 U.S. at 184–87.

Appellants do not argue the recited computer system implementing steps (A) through (C) operates in an unconventional manner or identified portions of the Specification to indicate that the computer system is unconventional. *See generally* Appeal Br. 41–46. The disclosure further describes the computer system in generalities. Spec. ¶¶ 41–44; Fig. 5. Using a generic computer for "determining," "designating," and "outputting" information simply takes advantage of some of the "most basic functions [of] a computer." *See Alice*, 134 S. Ct. at 2359 (the "use of a computer to obtain data, adjust account balances, and issue automated instructions; all of these computer functions are 'well-understood, routine, conventional activit[ies]' previously known to the industry") (quoting *Mayo*, 566 U.S. at 71–73); *see also Benson*, 409 U.S. at 65 (noting that a "computer operates then upon both new and previously stored data. The general-purpose computer is designed to perform operations under many different programs."). Thus, like the Examiner (Final Act. 10–11), we conclude the additional elements in claim 1 are no more than generic computer elements that do not transform the above-discussed abstract ideas into a patent-eligible invention.

To the extent the rejection found step (C) is not part of the abstract idea (*see* Final Act. 11), Appellants do not challenge that claim 1's step (C) outlined above is insignificant post-solution activity that does not add significantly more to the abstract ideas. Final Act. 11. As the Supreme Court has explained,

> [t]he notion that post-solution activity, no matter how conventional or obvious in itself, can transform an unpatentable principle into a patentable process exalts form over substance. A competent draftsman could attach some form of post-solution activity to almost any mathematical formula; the Pythagorean theorem would not have been patentable, or partially patentable, because a patent application contained a final step indicating that the formula, when solved, could be usefully applied to existing surveying techniques.

Flook, 437 U.S. at 589; *see also Diehr*, 450 U.S. at191–92 (observing insignificant post-solution activity "would allow a competent draftsman to evade the recognized limitations on the type of subject matter eligible for patent protection."); *Bilski v. Kappos*, 561 U.S. 593, 610–11 (2010); *Mayo*, 573 U.S. at 79. Thus, like the Examiner (Final Act. 11), we conclude step (C) outlined above is also insignificant post-solution activity.

To the extent Appellants argue "[j]ust as with the webpages of [*DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014)], there is no pre-Internet equivalent to group cyberattacks, which are limited to networks" (Appeal Br. 43), this argument is unavailing. Our reviewing court in *DDR Holdings* cautioned that "not all claims purporting to address Internet-centric challenges are eligible for patent." 773 F.3d at 1264 (referring to *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 715–16 (Fed. Cir. 2014)). Aside from being merely conclusory statements (*see* Appeal Br. 42–44), Appellants have not demonstrated persuasively that claim 1 contains a solution "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." *DDR Holdings*, 773 F.3d at 1257.

Appellants attempt to draw parallels between the claims in the instant application and *BASCOM Global Internet Services, Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed. Cir. 2016). *See* Appeal Br. 45–47. These arguments are unavailing. Aside from mere conclusory statements (*see* Appeal Br. 47), Appellants have not demonstrated persuasively that claim 1 contains a non-conventional or non-generic arrangement, whether considering the elements individually or as a combination.

To the extent Appellants attempt to draw parallels between the claims in the instant application and district court decisions (*see* Appeal Br. 47–48), these arguments are unavailing. We note that, although district court decisions may provide insightful analysis, we are not bound by such decisions.

Lastly, we note the Specification indicates techniques for detecting attacks by multiple attackers (e.g., botnets) by determining compromised network nodes, constructing graphs of network activity based on a rule set to detect suspicious network activity, and detecting coordinated attacks by using alert correlation are known. Spec. ¶¶ 3–7.

For the above reasons, claim 1's limitations, viewed "both individually and as an ordered combination," do not amount to significantly more than the judicial exception and do not sufficiently transform the nature of the claims into patent-eligible subject matter. *See Alice*, 134 S. Ct. at 2355.

Accordingly, Appellants have not persuaded us of error in the rejection of independent claim 1 and claims 2–5, 8–10, 12–17, 19, and 20, which are not separately argued.

DECISION

We affirm the Examiner's rejection of claims 1–5, 8–10, 12–17, 19, and 20 under 35 U.S.C. § 101.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 41.50(f).

AFFIRMED